1

Topics in representation theory of finite groups

Tullio Ceccherini-Silberstein, Fabio Scarabotti and Filippo Tolli

Abstract

This is an introduction to representation theory and harmonic analysis on finite groups. This includes, in particular, Gelfand pairs (with applications to diffusion processes *à la* Diaconis) and induced representations (focusing on the little group method of Mackey and Wigner). We also discuss Laplace operators and spectral theory of finite regular graphs. In the last part, we present the representation theory of $\mathrm{GL}(2,\mathbb{F}_q)$, the general linear group of invertible 2×2 matrices with coefficients in a finite field with q elements. More precisely, we revisit the classical Gelfand–Graev representation of $\mathrm{GL}(2,\mathbb{F}_q)$ in terms of the so-called multiplicity-free triples and their associated Hecke algebras. The presentation is not fully self-contained: most of the basic and elementary facts are proved in detail, some others are left as exercises, while, for more advanced results with no proof, precise references are provided.

Keywords: finite group, group representation, character, Gelfand pair, spherical function, spherical Fourier transform, Mackey–Wigner little group method, Markov chain, random walk, Ehrenfest diffusion process, ergodic theorem, finite graph, spectral graph theory, Laplace operator, distance-regular graph, strongly regular graph, association scheme, finite field, affine group over a finite field, general linear group over a finite field, Gelfand–Graev representation, multplicity-free triple, Hecke algebra

Mathematics Subject Classification: 20C15, 20C08, 20C30, 20C35, 20G05, 05C50, 43A35, 43A65, 43A30, 43A90

1.1 Introduction

The present text constitutes an expanded and more detailed exposition of the lecture notes of a course on Representation Theory delivered by the first named author at the International Conference and PhD-Master Summer School on Groups and Graphs, Designs and Dynamics (G2D2) held in Yichang (China) in August 2019.

One of the main features of Harmonic Analysis is the study of linear operators that are invariant with respect to the action of a group. In the classical abelian setting, for instance, this is used to express the solutions of a constant coefficients differential equation (such as the heat equation) in terms of infinite sums of exponentials (Fourier series).

Here, we consider a finite (possibly non-abelian) counterpart. Let G be a finite group, let $K \leq G$ be a subgroup, and consider the G-module $L(G/K)$ of all complex valued functions on the (finite) homogenous space G/K of left cosets of K in G. The corresponding space of linear G-invariant operators we alluded to above, the so-called commutant $\mathrm{End}_G(L(G/K))$, bears a natural structure of an involutive unital algebra that turns out to be isomorphic to the algebra ${}^K L(G)^K$ of all bi-K-invariant complex valued functions on G. When these algebras are commutative, we say that (G,K) is a Gelfand pair: the terminology originates from the seminal paper by I. M. Gelfand [40] in the setting of Lie groups. Finite Gelfand pairs, when G is a Weyl group or a Chevalley group over a finite field, or the symmetric group $S_n = \mathrm{Sym}(\{1,2,\dots,n\})$, were studied by Ph. Delsarte [25], motivated by applications to association schemes of coding theory, Ch F. Dunkl [30, 31, 32, 33] and D. Stanton [67] with relevant contributions to the theory of special functions, E. Bannai and T. Ito [3] who initiated Algebraic Combinatorics, J. Saxl [59] in the study of Finite Geometries and Designs, and A. Terras [69] with applications to number theory. A special mention deserves the work in Probability Theory by P. Diaconis and collaborators [26] with remarkable applications to the study of diffusion processes and asymptotic behaviour of finite Markov chains. A. Okounkov and A. M. Vershik [55] (see also [16]) used methods from the theory of finite Gelfand pairs in order to give a new approach to the representation theory of the symmetric groups. Further expositions of the theory of finite Gelfand pairs and association schemes can be found in the monographs by R. A. Bailey [2], P.-H. Zieschang [73], as well as in the survey paper [14] and in our first monograph [15]. We conclude this bibliographical overview by mentioning the work of R. I. Grigorchuk [43] (see also [5, 23, 24]) in connection with the theory of the so-called self-similar groups.

Given a Gelfand pair (G,K), the simultaneous diagonalization of all G-

invariant operators can be achieved by means of a particular basis of ${}^{K}L(G)^{K}$. The elements of this basis, called spherical functions, are the analogues of the exponentials in the classical case and can be defined both intrinsically and as matrix coefficients of particular representations (the spherical representations). Besides the trivial though interesting case when the group G is abelian, an important example of a Gelfand pair is given by $(G \times G, \widetilde{G})$, with $\widetilde{G}$ the diagonal subgroup: in this case, the spherical functions are nothing but the normalized characters of G, showing that the theory of central functions on a group can be treated in the setting of the Gelfand pairs, as a particular case.

By virtue of the Ergodic Theorem, the rate of convergence to the stationary distribution of the n-step distributions μ_n of a finite (ergodic and symmetric) Markov chain can be estimated in terms of the second largest eigenvalue modulus of the corresponding transition matrix. An example of a Gelfand pair is $(S_n, S_k \times S_{n-k})$, where $S_n = \mathrm{Sym}(\{1,2,\ldots,n\})$ is the symmetric group of degree n, and, for $1 \leq k \leq n/2$, we regard $S_k = \mathrm{Sym}(\{1,2,\ldots,k\})$ and $S_{n-k} = \mathrm{Sym}(\{k+1,k+2,\ldots,n\})$ as subgroups of S_n. In the 80s Diaconis and Shahshahani [28] (see also [14, 15]), were able to use this Gelfand pair to find very precise asymptotics of $(\mu_n)_{n\in\mathbb{N}}$ for the Bernoulli–Laplace model of diffusion. In particular, they showed that an interesting phenomenon occurs: the transition from order to chaos is concentrated in a relatively small interval of time: this is the *cut-off phenomenon*. Other important examples, where the theory of spherical functions plays a central role, are the Ehrenfest model of diffusion (see Section 1.5.2) and the random transpositions model [26, 27, 14, 15].

The G-module $L(G/K)$ can be seen as the representation space of the induced representation $\mathrm{Ind}_K^G \iota_K$ of the trivial representation ι_K of K, and we have that (G,K) is a Gelfand pair if and only if $\mathrm{Ind}_K^G \iota_K$ decomposes without multiplicity. More generally, if θ is an irreducible K-representation, the algebra $\mathrm{End}_G(\mathrm{Ind}_K^G \theta)$ of intertwiners is isomorphic to a suitable convolution algebra $\mathscr{H}(G,K,\theta)$ of complex valued functions on G, and we say that (G,K,θ) is a multiplicity-free triple if these algebras are commutative; equivalently, if $\mathrm{Ind}_K^G \theta$ decomposes without multiplicity. Multiplicity-free triples were partially studied by I. G. Macdonald [50], by D. Bump and D. Ginzburg [9], and in [19, Chapter 13] when $\dim\theta = 1$; a generalization to higher dimensions, with a complete analysis of the spherical functions, is treated in our papers [61, 62, 63, 64] and the recent monograph [20]. An earlier application, where a problem of Diaconis on the Bernoulli-Laplace diffusion model with many urns was solved, was presented in the second named author's PhD thesis and published in [60]. As pointed out in [19, Chapter 14], our theory of multiplicity-free triples shed light on the representation theory of $\mathrm{GL}(2,\mathbb{F}_q)$, the general linear group of 2×2 matrices with coefficients in the field with q elements, as developed by I. I. Piatetski-Shapiro in [57].

These lecture notes are organized as follows. In Section 1.2, we briefly recall the basics of the representation theory of finite groups: this includes Schur's lemma, some character theory, and the Peter–Weyl theorem. In Sections 1.2.2, 1.2.3, and 1.2.4 we study Gelfand pairs in detail, focusing on spherical functions, the spherical Fourier transform, and the harmonic analysis of invariant operators. Then, in Sections 1.5.1 and 1.5.2 we present the applications of Gelfand pairs to Markov chains, culminating in the celebrated Diaconis–Shahshahani upper-bound lemma, and describe the asymptotics for the Ehrenfest model of diffusion. In Sections 1.6.1 and 1.6.2 we study induced representations, Frobenius reciprocity, and Mackey theory, and then, in Section 1.6.3, we apply this machinery to obtain the Mackey–Wigner little group method. In Section 1.6.4 we introduce the Hecke algebras $\widetilde{\mathscr{H}}(G,K,\theta)$ and $\mathscr{H}(G,K,\theta)$ and show that they are both isomorphic to the commutant $\mathrm{End}_G(\mathrm{Ind}_K^G \theta)$. In Section 1.6.5 we then define multiplicity-free triples and present their general theory. After a short overview of the basics of finite fields and their characters (Section 1.7.1), as an application of the little group method of Mackey and Wigner we describe all irreducible representations of $\mathrm{Aff}(\mathbb{F}_q)$, the affine group over the field with q elements. The last two sections are devoted to the general linear group $\mathrm{GL}(2,\mathbb{F}_q)$ and its representations: in relation with the latter, we limit ourselves to the description of the decomposition of the Gelfand–Graev representation.

Our presentation is mostly self-contained. However, for the sake of brevity, some of the proofs are either omitted (but with clear references for a complete exposition), or sketched, or left as an exercise to the reader. Several other exercises are proposed as complements and further developments.

Acknowledgments. We express our deep gratitude to Yaokun Wu and Da Zhao for many valuable comments and remarks. We also thank Rosemary Bailey and Peter Cameron for their most precious help and concern in the editing process.

1.2 Representation theory and harmonic analysis on finite groups

In this section, we present the basics of the representation theory of finite groups and we introduce and study the notion of a finite Gelfand pair, thus providing a setting for a suitable extension of the classical Fourier analysis.

Our exposition is inspired by Diaconis' book [26] and to Figà–Talamanca's lecture notes [37] and our monographs [15, 19]. We also took a particular benefit from the monographs by Alperin and Bell [1], Fulton and Harris [39], Isaacs [46], Naimark and Stern [52], Serre [65], Simon [66], and Sternberg [68]. Expositions of the theory of Gelfand pairs are also presented in the monographs by J. Dieudonné [29], H. Dym and H. P. McKean [34] , J. Faraut [36], A. Figà-Talamanca and C. Nebbia [38], S. Helgason [44] and J. Wolf [71] for the general case of locally compact groups.

1.2.1 Representations

Let G be a finite group.

Definition 1.2.1 (Representation) A *representation* of G (also called a *G-representation*) is a pair (ρ, V), where V is a finite dimensional complex vector space and $\rho\colon G \to \mathrm{GL}(V)$ is a group homomorphism from G into the group $\mathrm{GL}(V)$ of all *invertible linear transformations* of V.

If (ρ, V) is a representation of G, then one has:

- $\rho(1_G) = I_V$
- $\rho(g_1 g_2) = \rho(g_1)\rho(g_2)$
- $\rho(g^{-1}) = \rho(g)^{-1}$
- $\rho(g)(av + bw) = a\rho(g)v + b\rho(g)w$

for all $g, g_1, g_2 \in G$, $v, w \in V$, and $a, b \in \mathbb{C}$, where $1_G \in G$ is the identity element and $I_V : V \to V$ is the identity transformation.

Equivalently, a representation can be viewed as an *action* $\alpha\colon G \times V \to V$ of G on V by linear transformations by setting $\alpha(g, v) := \rho(g)v$ for all $g \in G$ and $v \in V$.

In the following, for the sake of brevity, when a given representation (ρ, V) is clear from the context, we shall denote it simply by either ρ or V.

The dimension $d_\rho := \dim V$ of the vector space V is called the *dimension* of ρ.

Definition 1.2.2 (Sub-representation) Let (ρ, V) be a G-representation. A subspace $W \leq V$ is *G-invariant* if $\rho(g)w \in W$ for all $g \in G$ and $w \in W$. The pair (ρ_W, W), where $\rho_W(g) := \rho(g)|_W$ for all $g \in G$, is a G-representation, called a *sub-representation* of (ρ, V). We shall then write $(\rho_W, W) \leq (\rho, V)$.

Clearly, $d_{\rho_W} \leq d_\rho$.

Definition 1.2.3 (Irreducible representation) A G-representation (ρ, V) is *irreducible* if V admits no nontrivial G-invariant subspaces, that is, the only G-invariant subspaces $W \leq V$ are $W = \{0\}$ and $W = V$.

We denote by $\mathrm{Irr}(G)$ the set of all irreducible representations of G.

The representation of dimension zero is considered to be neither reducible nor irreducible, just as the number 1 is considered to be neither composite nor prime.

It is obvious that every one-dimensional representation is irreducible.

Definition 1.2.4 (Equivalent representations) Two G-representations (ρ_1, V_1) and (ρ_2, V_2) are *equivalent* if there exists a linear isomorphism $T\colon V_1 \to V_2$ such that

$$T \circ \rho_1(g) = \rho_2(g) \circ T$$

for all $g \in G$. We then write $\rho_1 \sim \rho_2$. We shall refer to T as to an *intertwining isomorphism*.

If (ρ_1, V_1) is equivalent to a sub-representation of (ρ_2, V_2) we write $\rho_1 \preceq \rho_2$, and we say that ρ_1 is *contained* in ρ_2.

Note that $\sim$ is an equivalence relation in the set of all G-representations, which preserves irreducibility and dimension (exercise).

Definition 1.2.5 (Unitary representation) Suppose that a complex vector space V is equipped with an inner product $\langle \cdot, \cdot \rangle_V$. A G-representation (ρ, V) is *unitary* if, for every $g \in G$, the linear operator $\rho(g)$ is unitary, that is,

$$\langle \rho(g)v_1, \rho(g)v_2 \rangle_V = \langle v_1, v_2 \rangle_V$$

for all $v_1, v_2 \in V$.

Note that, if (ρ, V) is a unitary representation, then

- $\rho(g^{-1}) = \rho(g)^*$

for all $g \in G$, where * denotes the *adjoint* operation.

Exercise 1.2.6 (Unitarizability of representations) Suppose that a complex vector space V is equipped with an inner product $\langle \cdot, \cdot \rangle_V$. Let (ρ, V) be a G-representation. Then when equipping V with the new inner product $(\cdot, \cdot)_V$ defined by

$$(v_1, v_2)_V := \frac{1}{|G|} \sum_{g \in G} \langle \rho(g)v_1, \rho(g)v_2 \rangle_V$$

for all $v_1, v_2 \in V$, the representation (ρ, V) becomes unitary.

By virtue of the previous exercise, from now on, we shall consider only unitary representations. This will not affect equivalence as the next exercise shows.

Exercise 1.2.7 Let (ρ_1, V_1) and (ρ_2, V_2) be two unitary G-representations. Suppose that $\rho_1 \sim \rho_2$. Then there exists a unitary operator $U\colon V_1 \to V_2$ such that

$$U \circ \rho_1(g) = \rho_2(g) \circ U$$

for all $g \in G$.

Hint: Use the *polar decomposition* $T = U|T|$ for an intertwining isomorphism $T\colon V_1 \to V_2$ (for more details, see [19, Lemma 10.1.4]).

We can rephrase the result in the above exercise by saying that two equivalent unitary representations are *unitarily equivalent*.

Definition 1.2.8 (Dual of a group) The *dual* of the group G is the quotient $\widehat{G} := \mathrm{Irr}(G)/\sim$. In the following we shall also refer to $\widehat{G}$ as to a complete set of irreducible pairwise non-equivalent G-representations.

We shall see later (cf. Theorem 1.2.36) that $|\widehat{G}| < \infty$.

Definition 1.2.9 (Direct sum) Let (ρ_1, V_1) and (ρ_2, V_2) be two G-representations. We equip $V := V_1 \oplus V_2$ with the inner product $\langle \cdot, \cdot \rangle_V$ defined by setting

$$\langle v_1 + v_2, v_1' + v_2' \rangle_V := \langle v_1, v_1' \rangle_{V_1} + \langle v_2, v_2' \rangle_{V_2}$$

for all $v_1, v_1' \in V_1$ and $v_2, v_2' \in V_2$. The (unitary) G-representation (ρ, V) defined by setting

$$\rho(g)(v_1 + v_2) := \rho_1(g)v_1 + \rho_2(g)v_2$$

for all $g \in G$ and $v_1 \in V_1$, $v_2 \in V_2$, is called the *direct sum* of (ρ_1, V_1) and (ρ_2, V_2) and is denoted by $(\rho_1 \oplus \rho_2, V_1 \oplus V_2)$.

Note that $d_{\rho_1 \oplus \rho_2} = d_{\rho_1} + d_{\rho_2}$ and that $\rho_i \preceq \rho_1 \oplus \rho_2$ for $i = 1, 2$.

Definition 1.2.10 (Conjugate representation) Let (ρ, V) be a G-representation and let V' denote the dual vector space. The *conjugate representation* of ρ is the unitary representation (ρ', V') defined by setting

$$[\rho'(g)f](v) := f(\rho(g^{-1})v)$$

for all $g \in G$, $f \in V'$, and $v \in V$.

It is an exercise to check that ρ' is unitary (resp. irreducible) if and only if ρ is unitary (resp. irreducible).

https://doi.org/10.1017/9781009465939.002 Published online by Cambridge University Press

Exercise 1.2.11 (Orthogonal complement) Suppose that (ρ, V) is a (unitary) G-representation and let $W \leq V$ be a nontrivial G-invariant subspace. Show that

$$W^{\perp} = \{v \in V : \langle v, w \rangle_V = 0 \text{ for all } w \in W\}$$

is also G-invariant. Deduce that $\rho = \rho_W \oplus \rho_{W^{\perp}}$.

From the above exercise and an obvious inductive argument, one immediately deduces the following:

Theorem 1.2.12 *Every G-representation is the direct sum of finitely many irreducible G-representations.* □

The above theorem may be rephrased as follows. Suppose that (ρ, V) is a G-representation. Then there exist a positive integer n and (not necessarily distinct) $\rho_1, \rho_2, \ldots, \rho_n \in \widehat{G}$ such that $\rho \sim \rho_1 \oplus \rho_2 \oplus \cdots \oplus \rho_n$.

Example 1.2.13 (Trivial representation) The *trivial representation* of a group G, denoted $(\iota_G, \mathbb{C})$, is the one-dimensional representation defined by setting $\iota_G(g) = \mathrm{Id}_{\mathbb{C}}$ for all $g \in G$.

Given a finite group G, we denote by $L(G)$ the complex vector space of all functions $f\colon G \to \mathbb{C}$. We equip $L(G)$ with the *convolution product* $*$ defined by setting, for $f_1, f_2 \in L(G)$,

$$(f_1 * f_2)(g) = \sum_{h \in G} f_1(gh^{-1}) f_2(h) \quad \text{for all } g \in G. \tag{1.1}$$

With the product $*$, the space $L(G)$ becomes an algebra, called the $\mathbb{C}$-*group algebra* of G. Note that $L(G)$ is unital, with unity element δ_{1_G}. Moreover, the map $f \mapsto f^*$, where $f^*(g) := \overline{f(g^{-1})}$ for all $g \in G$, is an involution.

Example 1.2.14 (Regular representations) Let G be a finite group. Then the *left* (resp. *right*) *regular representation* of G is the (unitary) representation $(\lambda_G, L(G))$ (resp. $(\rho_G, L(G))$) defined by setting

$$[\lambda_G(g)f](h) = f(g^{-1}h) \quad (\text{resp. } [\rho_G(g)f](h) = f(hg))$$

for all $g, h \in G$ and $f \in L(G)$.

Exercise 1.2.15 Show that the left (resp. right) regular representation is unitary when $L(G)$ is endowed with the scalar product $\langle \cdot, \cdot \rangle_{L(G)}$ defined by setting

$$\langle f_1, f_2 \rangle_{L(G)} := \sum_{g \in G} f_1(g) \overline{f_2(g)}$$

for all $f_1, f_2 \in L(G)$.

https://doi.org/10.1017/9781009465939.002 Published online by Cambridge University Press

Example 1.2.16 (Representations of a cyclic group) Let

$$G = C_n = \{1, a, a^2, \dots, a^{n-1}\} \cong \mathbb{Z}/n\mathbb{Z}$$

denote the *cyclic group* of order n. Consider the primitive nth root of unity $\omega := e^{2\pi i/n}$ and, for $k \in \mathbb{Z}$, let $(\rho_k, \mathbb{C})$ denote the (unitary) representation defined by

$$\rho_k(a^h) = \omega^{kh}\mathrm{Id}_{\mathbb{C}}$$

for all $h = 0, 1, \dots, n-1$. Note that $\rho_k = \rho_{k'}$ if $k \equiv k' \bmod n$ and that $\rho_k \not\sim \rho_{k'}$ if $k \not\equiv k' \bmod n$. In fact, $\widehat{C_n} = \{\rho_k : k = 0, 1, \dots, n-1\}$.

Example 1.2.17 (Two particular representations of the symmetric group) Let $G = S_n = \mathrm{Sym}(\{1, 2, \dots, n\})$ denote the *symmetric group* of degree n, that is the group of all bijective maps (*permutations*) $g\colon \{1, 2, \dots, n\} \to \{1, 2, \dots, n\}$.

The *sign representation* of S_n is the one-dimensional representation $(\mathrm{sign}, \mathbb{C})$ defined by

$$\mathrm{sign}(g) = \begin{cases} \mathrm{Id}_{\mathbb{C}} & \text{if } g \in A_n \\ -\mathrm{Id}_{\mathbb{C}} & \text{if } g \in S_n \setminus A_n \end{cases}$$

for all $g \in S_n$, where $A_n \leq S_n$ is the *alternating subgroup* (consisting of all permutations which can be expressed as a product of an even number of transpositions).

Let V be an n-dimensional vector space equipped with a scalar product. Fix an orthonormal basis $\{e_1, e_2, \dots, e_n\} \subset V$. The *permutation representation* of S_n (cf. Definition 1.2.50) is the (unitary) representation (ρ, V) defined by setting

$$\rho(g)e_i = e_{g(i)}$$

for all $g \in S_n$ and $i = 1, 2, \dots, n$.

Exercise 1.2.18 Let $G = S_n$ be the symmetric group of degree n.

Show that the sign representation $(\mathrm{sign}, \mathbb{C})$ is indeed a unitary representation.

Show that the permutation representation (ρ, V) is indeed a unitary representation. Let $W \leq V$ denote the one-dimensional subspace spanned by the vector $e_1 + e_2 + \cdots + e_n$. Show that W is G-invariant. Show that

$$W^\perp = \{\sum_{i=1}^{n} \alpha_i e_i : \alpha_i \in \mathbb{C} \text{ and } \alpha_1 + \alpha_2 + \cdots + \alpha_n = 0\}$$

is equal to the linear span of $\{e_i - e_{i-1} : i = 2, 3, \dots, n\}$, and is irreducible. Deduce that $V = W \oplus W^\perp$ is the decomposition of V into irreducible components.

Definition 1.2.19 (Commutant) The *commutant* of two G-representations (ρ_1, V_1) and (ρ_2, V_2) is the vector space

$$\mathrm{Hom}_G(V_1, V_2) := \{T\colon V_1 \to V_2 : T \text{ is linear and } T\rho_1(g) = \rho_2(g)T \text{ for all } g \in G\}.$$

We refer to its elements as to the *intertwiners* of ρ_1 and ρ_2. When $V_1 = V_2 = V$ we denote the *commutant* $\mathrm{Hom}_G(V,V)$ by $\mathrm{End}_G(V)$. It has a natural structure of an algebra.

Exercise 1.2.20 Let (ρ_1, V_1), (ρ_2, V_2), and (ρ, V) be unitary G-representations. Given $T \in \mathrm{Hom}_G(V_1, V_2)$, let $T^*\colon V_2 \to V_1$ denote the adjoint operator. Show that $T^* \in \mathrm{Hom}_G(V_2, V_1)$. Show that the commutant $\mathrm{End}_G(V)$ has a natural structure of a $*$-algebra.

The following is a celebrated, elementary but extremely useful result of Schur.

Lemma 1.2.21 (Schur's lemma) *Let (ρ_1, V_1) and (ρ_2, V_2) be two irreducible G-representations. If $T \in \mathrm{Hom}_G(V_1, V_2)$, then either $T = 0$ or T is an isomorphism (and $\rho_1 \sim \rho_2$).*

Proof The kernel $\ker T \le V_1$ and the image $\mathrm{ran}\, T \le V_2$ are G-invariant subspaces, and by the irreducibility of ρ_1 and ρ_2 they must be trivial. If $\ker T = \{0\}$, then $\mathrm{ran}\, T = V_2$ and therefore T is an isomorphism; and if $\ker T = V_1$, then $T \equiv 0$. □

Corollary 1.2.22 *Let (ρ, V) be an irreducible G-representation and consider $T \in \mathrm{End}_G(V)$. Then $T \in \mathbb{C}I_V$.*

Proof Let $\lambda \in \mathbb{C}$ be an eigenvalue of T, so that $T - \lambda I_V$ cannot be an isomorphism. As $T - \lambda I_V \in \mathrm{End}_G(V)$, Schur's lemma (Lemma 1.2.21) ensures that $T - \lambda I_V \equiv 0$, that is, $T = \lambda I_V$. □

Exercise 1.2.23 Let G be a group. Show that if G is abelian and (ρ, V) is a G-representation, then ρ is irreducible if and only if $d_\rho = 1$. Show that, vice versa, if every irreducible G-representation is one-dimensional, then G is abelian.
Hint. For the converse implication, use the following steps:

- A representation (ρ, V) of G is *faithful* provided that $\rho(g) \neq I_V$ for all $g \in G \setminus \{1_G\}$. Show that the regular representations (cf. Example 1.2.14) of G are faithful.
- Apply Theorem 1.2.12 to the left regular representation of G and deduce that for every $g \in G \setminus \{1_G\}$, there exists an irreducible representation (ρ_g, V_g) of G such that $\rho_g(g) \neq I_V$.

- If G is nonabelian, there exist $g_1, g_2 \in G$ such that $g_1 g_2 \neq g_2 g_1$. Use the previous step, with $g = g_1 g_2 g_1^{-1} g_2^{-1} \neq 1_G$ to show that (ρ_g, V_g) cannot be one-dimensional.

For an alternative solution, see Remark 1.2.43.

Definition 1.2.24 (Matrix coefficient) Let (ρ, V) be a G-representation and $v, w \in V$. The *matrix coefficient* associated with the pair (v, w) is the function $u^\rho_{v,w} \colon G \to \mathbb{C}$ defined by setting

$$u^\rho_{v,w}(g) = \langle \rho(g) w, v \rangle_V \quad \text{for all } g \in G.$$

If $\{v_1, v_2, \ldots, v_{d_\rho}\}$ is a basis of V, the matrix coefficient $u^\rho_{v_i, v_j}$ will be simply denoted by $u^\rho_{i,j}$. Observe that the matrix $(u^\rho_{i,j})_{i,j}$ is the matrix representing the operator $\rho(g) \in \mathrm{End}(V)$ with respect to the basis $\{v_1, v_2, \ldots, v_{d_\rho}\}$.

Lemma 1.2.25 (Orthogonality relations) *Let (ρ_1, V_1) and (ρ_2, V_2) be two irreducible G-representations and suppose that $\rho_1 \not\sim \rho_2$. Then every matrix coefficient of ρ_1 is orthogonal to every matrix coefficient of ρ_2.*

Proof Let $v_1, w_1 \in V_1$ and $v_2, w_2 \in V_2$ and define

$$\begin{array}{rccc} L\colon & V_1 & \longrightarrow & V_2 \\ & v & \mapsto & \langle v, w_1 \rangle_{V_1} w_2 \end{array}$$

and

$$\tilde{L} = \sum_{g \in G} \rho_2(g^{-1}) L \rho_1(g).$$

It is easy to check that $\tilde{L}$ belongs to $\mathrm{Hom}_G(V_1, V_2)$ so that, by Schur's lemma, $\tilde{L} = 0$. Thus

$$\begin{aligned} 0 = \langle \widetilde{L} v_1, v_2 \rangle_{V_2} &= \sum_{g \in G} \langle L \rho_1(g) v_1, \rho_2(g) v_2 \rangle_{V_2} \\ &= \sum_{g \in G} \langle \rho_1(g) v_1, w_1 \rangle_{V_1} \langle w_2, \rho_2(g) v_2 \rangle_{V_2} \\ &= \sum_{g \in G} u^{\rho_1}_{w_1, v_1}(g) \overline{u^{\rho_2}_{w_2, v_2}(g)} \\ &= \langle u^{\rho_1}_{w_1, v_1}, u^{\rho_2}_{w_2, v_2} \rangle_{L(G)}. \end{aligned}$$

This shows that the matrix coefficients $u^{\rho_1}_{w_1, v_1}$ and $u^{\rho_2}_{w_2, v_2}$ are orthogonal. $\square$

Lemma 1.2.26 *Let (ρ, V) be an irreducible G-representation. If $\{v_1, \ldots, v_{d_\rho}\}$ is an orthonormal basis of V, then one has*

$$\langle u^\rho_{i,j}, u^\rho_{k,\ell} \rangle_{L(G)} = \frac{|G|}{d_\rho} \delta_{i,k} \delta_{j,\ell}$$

for all $1 \le i, j, k, \ell \le d_\rho$.

Proof We leave the proof as an exercise as a slight modification of the previous one. Note that in the present setting we have $\widetilde{L} \in \mathbb{C}I_V$. □

Exercise 1.2.27 Let (ρ, V) be a (not necessarily irreducible) G-representation and fix an orthonormal basis $\{v_1, \ldots, v_{d_\rho}\}$ of V. Show that:

- $u^\rho_{i,j}(g^{-1}) = \overline{u^\rho_{j,i}(g)}$;
- $u^\rho_{i,j}(g_1 g_2) = \sum_{k=1}^{d_\rho} u^\rho_{i,k}(g_1) u^\rho_{k,j}(g_2)$;
- $\sum_{j=1}^{d_\rho} u^\rho_{j,i}(g)\overline{u^\rho_{j,k}(g)} = \delta_{i,k}$ (*dual orthogonality relations*);

for all $g, g_1, g_2 \in G$ and $1 \le i, j, k \le d_\rho$.

Let V be a finite dimensional vector space. We recall that the *trace* is the linear map $\mathrm{tr}\colon \mathrm{End}(V) \to \mathbb{C}$ that satisfies the following two properties:

(T1) $\mathrm{tr}(xy) = \mathrm{tr}(yx)$ for all $x, y \in \mathrm{End}(V)$
(T2) $\mathrm{tr}(I_V) = \dim V$.

Note that if $\{v_1, v_2, \ldots, v_d\}$ is an orthogonal basis of V, then $\mathrm{tr}(x) = \sum_{i=1}^{d} \langle xv_i, v_i\rangle_V$ for all $x \in \mathrm{End}(V)$.

Definition 1.2.28 The *character* of a G-representation (ρ, V) is the map $\chi^\rho : G \to \mathbb{C}$ defined by setting

$$\chi^\rho(g) = \mathrm{tr}(\rho(g)) = \sum_{i=1}^{d_\rho} u^\rho_{i,i}(g)$$

for all $g \in G$, where, for the last term, the diagonal matrix coefficients are relative to an (= any) orthonormal basis of V.

Remark 1.2.29 Let ρ, σ be G-representations. We denote the unitary group of complex numbers by $\mathbb{T} = \{z \in \mathbb{C} : |z| = 1\} \subset \mathbb{C}$. Then:

- If $d_\rho = 1$, then $\chi^\rho \equiv \rho : G \to \mathbb{T}$;
- if $\rho \sim \sigma$, then $\chi^\rho = \chi^\sigma$ (cf. Corollary 1.2.35);
- $\chi^\rho(1_G) = d_\rho$;
- $\chi^\rho(ghg^{-1}) = \chi^\rho(h)$;
- $\chi^\rho(g^{-1}) = \overline{\chi^\rho(g)}$,

for all $g, h \in G$.

Exercise 1.2.30 Show that $|\chi^\rho(g)| \le d_\rho$ for all $g \in G$.

Corollary 1.2.31 *Let ρ_1 and ρ_2 be two irreducible G-representations. Then*

$$\langle \chi^{\rho_1}, \chi^{\rho_2} \rangle_{L(G)} = \begin{cases} |G| & \textit{if } \rho_1 \sim \rho_2 \\ 0 & \textit{otherwise}. \end{cases}$$

In other words, the characters constitute an orthogonal system in $L(G)$. □

Corollary 1.2.32 *Let ρ and σ be two G-representations. Suppose that $\rho = \rho_1 \oplus \rho_2 \oplus \cdots \oplus \rho_k$ is a decomposition of ρ into irreducible representations and that σ is irreducible. Then, setting $m_\sigma^\rho := |\{i : \sigma \sim \rho_i\}|$, we have that*

$$m_\sigma^\rho = \frac{1}{|G|} \langle \chi^\rho, \chi^\sigma \rangle_{L(G)}.$$ □

Definition 1.2.33 The (nonnegative) integer m_σ^ρ is called the *multiplicity of σ in ρ*.

Corollary 1.2.34 *Let ρ and σ be two G representations. Suppose that $\rho \sim \oplus_{\theta \in \widehat{G}} m_\theta^\rho \theta$ and $\sigma \sim \oplus_{\theta \in \widehat{G}} m_\theta^\sigma \theta$. Then*

$$\frac{1}{|G|} \langle \chi^\rho, \chi^\sigma \rangle_{L(G)} = \sum_{\theta \in \widehat{G}} m_\theta^\rho m_\theta^\sigma.$$ □

Corollary 1.2.35 *Let ρ and σ be two G-representations. Then*

- *ρ is irreducible if and only if $\frac{1}{|G|} \langle \chi^\rho, \chi^\rho \rangle_{L(G)} = 1$;*
- *$\rho \sim \sigma$ if and only if $\chi^\rho = \chi^\sigma$.* □

The following is a fundamental result on the representation theory of finite groups: it provides a complete description of the decomposition of the regular representation. It was proved, in the more general setting of compact groups, by Hermann Weyl and his student Fritz Peter [56].

Theorem 1.2.36 (Peter–Weyl) (1) *Every irreducible representation $(\rho, V_\rho) \in \widehat{G}$ appears in the left regular representation $(\lambda_G, L(G))$ with multiplicity equal to its dimension:*

$$L(G) \sim \bigoplus_{\rho \in \widehat{G}} d_\rho V_\rho.$$

(2) *The set $\mathfrak{U} = \{u_{i,j}^\rho : 1 \leq i, j \leq d_\rho, \rho \in \widehat{G}\}$ of matrix coefficients is a complete orthogonal system in $L(G)$.*

(3) $|G| = \sum_{\rho \in \widehat{G}} d_\rho^2$.

https://doi.org/10.1017/9781009465939.002 Published online by Cambridge University Press

Proof (1) Let $g,h \in G$. Since $\lambda_G(g)\delta_h = \delta_{gh}$ we have

$$\chi^{\lambda_G}(g) = \begin{cases} |G| & \text{if } g = 1_G \\ 0 & \text{otherwise.} \end{cases}$$

Therefore, if $\rho \in \widehat{G}$ the multiplicity of ρ in λ_G is given by

$$m_\rho^{\lambda_G} = \frac{1}{|G|}\langle \chi^\rho, \chi^{\lambda_G}\rangle_{L(G)} = \frac{1}{|G|}\sum_{g\in G}\chi^\rho(g)\chi^{\lambda_G}(g) = \chi^\rho(1_G) = d_\rho.$$

(2) and (3) follow easily by observing that $|G| = \dim L(G) = \sum_{\rho\in\widehat{G}} d_\rho^2$ and $|\mathfrak{U}| = \sum_{\rho\in\widehat{G}} d_\rho^2$. □

Definition 1.2.37 Let G be a finite group. A function $f \in L(G)$ is said to be *central* if the following equivalent conditions hold:

(1) f is constant on each *conjugacy class* $\mathscr{C}(g) := \{h^{-1}gh : h \in G\}$, $g \in G$, of G;
(2) $f(gh) = f(hg)$ for all $g,h \in G$;
(3) $f * f' = f' * f$ for all $f' \in L(G)$.

Exercise 1.2.38 Let G be a finite group.

(1) Show that the conditions (1), (2), and (3) in Definition 1.2.37 are equivalent.
(2) Show that the set $\mathscr{A}$ of all central functions in $L(G)$ forms a $*$-subalgebra.
(3) Show that $f * \phi * f^* \in \mathscr{A}$ for all $f \in L(G)$ and $\phi \in \mathscr{A}$.
(4) Show that $\chi^\rho \in \mathscr{A}$ for all G-representations ρ.

Theorem 1.2.39 *The characters constitute an orthogonal basis of the vector space of central functions of $L(G)$. In particular, $|\widehat{G}|$ equals the number of conjugacy classes of G.*

Proof See [15, Theorem 3.9.10] and/or [19, Theorem 10.3.13.(ii)]. □

Definition 1.2.40 Let G be a finite group. A function $\phi\colon G \to \mathbb{C}$ is said to be *positive-definite* if the following equivalent conditions hold:

(1) $\sum_{g,h\in G}\phi(h^{-1}g)f(g)\overline{f(h)} \geq 0$ for all $f \in L(G)$;
(2) $\sum_{i,j=1}^n c_i\overline{c_j}\phi(g_j^{-1}g_i) \geq 0$ for all $c_1,c_2,\ldots,c_n \in \mathbb{C}$, $g_1,g_2,\ldots,g_n \in G$, and $n \geq 1$;
(3) there exists a (unitary) representation (σ_ϕ, V_ϕ) of G and a cyclic vector $v_\phi \in V_\phi$ such that $\phi(g) = \langle\sigma_\phi(g)v_\phi, v_\phi\rangle_{V_\phi}$ for all $g \in G$.

In condition (3) above, the vector $v_\phi \in V_\phi$ being *cyclic* means that the vectors $\sigma_\phi(g)v_\phi$, $g \in G$, span V_ϕ.

Exercise 1.2.41 Let G be a finite group.

(1) Show that the conditions (1), (2), and (3) in Definition 1.2.40 are equivalent.
(2) Show that a linear combination with positive coefficients of positive-definite functions is positive-definite as well.
(3) Show that characters of G-representations are positive-definite functions.

Hint. For the implication (1) $\implies$ (3), define $\widetilde{\phi}\colon L(G) \to \mathbb{C}$ by setting

$$\widetilde{\phi}(f) := \sum_{g\in G} \phi(g)f(g)$$

for all $f \in L(G)$, and define $\ll\cdot,\cdot\gg\colon L(G) \times L(G) \to \mathbb{C}$ by setting

$$\ll f_1, f_2\gg \ := \widetilde{\phi}(f_2^* * f_1) \equiv \sum_{g,h\in G} \phi(h^{-1}g)f_1(g)\overline{f_2(h)}$$

for all $f_1, f_2 \in L(G)$. Show that $\ll\cdot,\cdot\gg$ defines a semi-definite sesquilinear form on $L(G)$. Show that the degenerate elements $f \in L(G)$ which satisfy $\ll f, f\gg\ = 0$ form a left ideal $\mathscr{I}$ of $L(G)$. The quotient space $V_\phi := L(G)/\mathscr{I}$ is a complex vector space with an inner product defined by setting

$$\langle f_1 + \mathscr{I}, f_2 + \mathscr{I}\rangle_{V_\phi} := \ll f_1, f_2 \gg$$

for all $f_1, f_2 \in L(G)$: check that the above is well defined.

Finally, define the G-representation (σ_ϕ, V_ϕ) by setting

$$\sigma_\phi(g)(f + \mathscr{I}) := \lambda_G(g)f + \mathscr{I}$$

for all $g \in G$ and $f \in L(G)$, where λ_G is the left-regular representation of G, and set

$$v_\phi := \delta_{1_G} + \mathscr{I} \in V_\phi,$$

where $\delta_{1_G} \in L(G)$ is the Dirac function at the identity element 1_G of G.

The triple $(V_\phi, \sigma_\phi, v_\phi)$ above is called the *GNS-construction*, after Israel M. Gelfand, Mark A. Naimark, and Irving E. Segal.

The following is a finite group version of a celebrated theorem of Salomon Bochner stating that the finite positive Borel probability measures on a locally compact abelian group G (e.g., $G = \mathbb{R}$) are the Fourier transform of continuous positive-definite functions on the Pontryagin dual $\widehat{G}$ of G (note that $\widehat{\mathbb{R}} \cong \mathbb{R}$) which take value 1 at $1_{\widehat{G}}$ (cf. [58, Theorem IX.9]).

Proposition 1.2.42 *Let G be a finite group and let $\phi \in L(G)$. Then the following conditions are equivalent:*

(1) *ϕ is central, positive-definite, and $\phi(1_G) = 1$;*

https://doi.org/10.1017/9781009465939.002 Published online by Cambridge University Press

(2) *there exists* $(\alpha_\sigma)_{\sigma\in\widehat{G}}$, *where* $\alpha_\sigma \in [0,1]$ *and* $\sum_{\sigma\in\widehat{G}} \alpha_\sigma = 1$, *such that*

$$\phi = \sum_{\sigma\in\widehat{G}} \frac{\alpha_\sigma}{d_\sigma}\chi^\sigma.$$

Proof This is left as an exercise (see also [7, Proposition 1.6]). □

Condition (2) above may be rephrased by saying that ϕ is a convex combination of normalized characters.

Remark 1.2.43 Let G be a group such that $d_\rho = 1$ for all $(\rho, V) \in \widehat{G}$. It follows from Theorem 1.2.36.(2) and Theorem 1.2.39 that $L(G)$ is a commutative algebra. The latter is easily seen to be equivalent to G being abelian. This constitutes an alternative (more advanced) solution to Exercise 1.2.23.

Definition 1.2.44 Let V_1 and V_2 be two complex vector spaces endowed with scalar products. Their *tensor product* $V_1 \otimes V_2$ is the linear span of $\{v_1 \otimes v_2 : v_1 \in V_1, v_2 \in V_2\}$, where $v_1 \otimes v_2$ denotes the anti-bilinear form on $V_1 \times V_2$ defined by setting

$$(v_1 \otimes v_2)(u_1, u_2) = \langle v_1, u_1\rangle_{V_1} \langle v_2, u_2\rangle_{V_2}$$

for all $(u_1, u_2) \in V_1 \times V_2$. We equip $V_1 \otimes V_2$ with the scalar product defined by

$$\langle v_1 \otimes v_2, w_1 \otimes w_2\rangle := \langle v_1, w_1\rangle_{V_1} \langle v_2, w_2\rangle_{V_2} \quad \text{for all } v_1, w_1 \in V_1, v_2, w_2 \in V_2.$$

If $A_i \in \mathrm{End}(V_i)$, $i = 1,2$, we define their tensor product $A_1 \otimes A_2 \in \mathrm{End}(V_1 \otimes V_2)$ by setting $(A_1 \otimes A_2)(v_1 \otimes v_2) = (A_1 v_1) \otimes (A_2 v_2)$ for all $v_1 \in V_1$ and $v_2 \in V_2$.

Let (ρ_1, V_1) (resp. (ρ_2, V_2)) be a representation of a group G_1 (resp. G_2). Their *outer tensor product* is the $(G_1 \times G_2)$-representation $(\rho_1 \boxtimes \rho_2, V_1 \otimes V_2)$ defined by setting

$$(\rho_1 \boxtimes \rho_2)(g_1, g_2) = \rho_1(g_1) \otimes \rho_2(g_2) \quad \text{for all } (g_1, g_2) \in G_1 \times G_2.$$

Similarly, if (ρ_1, V_1) and (ρ_2, V_2) are two representations of the same group G, their *internal tensor product* is the G-representation $(\rho_1 \otimes \rho_2, V_1 \otimes V_2)$ defined by setting

$$(\rho_1 \otimes \rho_2)(g) = \rho_1(g) \otimes \rho_2(g) \quad \text{for all } g \in G.$$

After identifying G with the diagonal subgroup $\widetilde{G} = \{(g,g) : g \in G\}$ of $G \times G$, we observe that $\rho_1 \otimes \rho_2 = \mathrm{Res}^{G\times G}_{\widetilde{G}}(\rho_1 \boxtimes \rho_2)$.

Exercise 1.2.45 Let ρ_1, ρ_1' (resp. ρ_2, ρ_2') be two G_1 (resp. G_2)-representations. Show that

(1) $\chi^{\rho_1 \boxtimes \rho_2}(g_1, g_2) = \chi^{\rho_1}(g_1)\chi^{\rho_2}(g_2)$ for all $(g_1, g_2) \in G_1 \times G_2$;

https://doi.org/10.1017/9781009465939.002 Published online by Cambridge University Press

(2) $\rho_1 \boxtimes \rho_2$ is irreducible if and only if ρ_1 and ρ_2 are irreducible;
(3) $\rho_1 \boxtimes \rho_2 \sim \rho_1' \boxtimes \rho_2'$ if and only if $\rho_1 \sim \rho_1'$ and $\rho_2 \sim \rho_2'$.

From the above exercise one deduces the following:

Theorem 1.2.46 *Let G_1 and G_2 be two groups. Then $\widehat{G_1 \times G_2} = \widehat{G_1} \boxtimes \widehat{G_2}$.* □

Exercise 1.2.47 Let (ρ, V) be a unitary representation of a group G and let (ρ', V') be its conjugate representation (cf. Definition 1.2.10). Show that the trivial representation of G (cf. Definition 1.2.13) satisfies $\iota_G \preceq \rho \otimes \rho'$.

If A is a (finite) abelian group, then there exist $d_1, d_2, \ldots, d_n \in \mathbb{N}$ with $d_i | d_{i+1}$, $i = 1, 2, \ldots, n-1$ such that $A \cong C_{d_1} \times C_{d_2} \times \cdots \times C_{d_n}$ (recall that $C_d \cong \mathbb{Z}/d\mathbb{Z}$ is the cyclic group of order d). The dual of an abelian group has a natural structure of an abelian group and we have

$$\widehat{A} \cong \widehat{C_{d_1}} \times \widehat{C_{d_2}} \times \cdots \times \widehat{C_{d_n}} \cong C_{d_1} \times C_{d_2} \times \cdots \times C_{d_n} \cong A.$$

The group isomorphism $A \cong \widehat{A}$ is not canonical, but we have the canonical *Pontryagin duality* between A and its *bidual* (the dual of the dual) $\widehat{\widehat{A}}$:

$$A \ni g \mapsto \psi_g \in \widehat{\widehat{A}}, \quad \text{with } \psi_g(\chi) = \chi(g) \quad \text{for all } \chi \in \widehat{A}.$$

1.2.2 Finite Gelfand pairs

Let G be a finite group and let $K \leq G$ be a subgroup.

A function $f \in L(G)$ is *K-invariant* on the *right* (resp. on the *left*) if $f(gk) = f(g)$ (resp. $f(kg) = f(g)$) for all $g \in G$ and $k \in K$. Then f is *bi-K-invariant* if it is K-invariant both on the left and the right. We denote by $L(G)^K$ (resp. ${}^K L(G)$) the subspace of $L(G)$ of K-invariant functions on the right (resp. on the left).

Let $X = G/K = \{gK : g \in G\}$ be the *homogeneous space* of *left cosets* of K in G and observe that we can identify $L(G)^K$ with $L(X) = \{f : X \to \mathbb{C}\}$: indeed, the map $L(X) \ni f \mapsto \widetilde{f} \in L(G)^K$, defined by

$$\widetilde{f}(g) := f(gK) \quad \text{for all } g \in G$$

yields a linear isomorphism from $L(X)$ onto $L(G)^K$.

More generally, suppose that G acts transitively on a set X (that is, for all $x_1, x_2 \in X$ there exists $g \in G$ such that $gx_1 = x_2$; equivalently, for all $x \in X$ the *G-orbit* $Gx := \{gx : g \in G\}$ of x is all of X). Fix $x_0 \in X$ and denote by $K = \mathrm{Stab}_G(x_0) := \{g \in G : gx_0 = x_0\}$ the *stabilizer* of x_0 in G. Then the map $X \ni gx_0 \mapsto gK \in G/K$ is a bijection.

Similarly, if $K\backslash G/K = \{KgK : g \in G\}$ denotes the set of *double cosets* of K in G, then the space of bi-K-invariant functions

$$^{K}L(G)^{K} := \{f \in L(G) : f(k_1 g k_2) = f(g), \forall k_1, k_2 \in K,\ g \in G\}$$

is isomorphic to both $L(K\backslash G/K)$ and

$$^{K}L(X) := \{f \in L(X) : f(kx) = f(x), \text{ for all } x \in X \text{ and } k \in K\};$$

the second isomorphism is given, again, by the map $f \mapsto \widetilde{f}$ restricted to $^{K}L(X)$.

Note that if $f_1, f_2 \in L(X)$, then

$$\langle f_1, f_2 \rangle_{L(X)} = \frac{1}{|K|} \langle \widetilde{f_1}, \widetilde{f_2} \rangle_{L(G)}.$$

Exercise 1.2.48 Let G act transitively on a set X. Consider the diagonal action of G on $X \times X$ given by $g(x_1, x_2) := (gx_1, gx_2)$ for all $g \in G$ and $x_1, x_2 \in X$. Fix $x_0 \in X$ and let $K = \mathrm{Stab}_G(x_0)$. Show that the following quantities are all equal:

(1) the number of G-orbits on $X \times X$;
(2) the number of K-orbits on X;
(3) $|K\backslash G/K|$.

Hint. Show that the map that associates with a G-orbit Θ on $X \times X$ the subset $\Omega := \{x \in X : (x, x_0) \in \Theta\}$ yields a bijection between the set of all G-orbits on $X \times X$ and the set of all K-orbits on X. Also show that the map $KgK \mapsto Kgx_0$ yields a bijection between the set of all double cosets of K in G and the set of all K-orbits on X.

Exercise 1.2.49 (1) Show that for $f_1, f_2 \in L(G)$ we have that $f_1 * f_2$ is K-invariant on the left (resp. right) if f_1 (resp. f_2) is K-invariant on the left (resp. right). Deduce that $^{K}L(G)^{K}$ is a two-sided ideal of $L(G)$.

(2) Check that the map $L(G) \ni f \mapsto f^K \in L(G)^K$, with

$$f^K(g) := \frac{1}{|K|} \sum_{k \in K} f(gk),\ \forall g \in G$$

is well defined and it is the orthogonal projection onto the subspace of right K-invariant functions.

(3) Check that the map $L(G) \ni f \mapsto {}^{K}f^{K} \in {}^{K}L(G)^{K}$, with

$$^{K}f^{K}(g) := \frac{1}{|K|^2} \sum_{k_1, k_2 \in K} f(k_1 g k_2),\ \forall g \in G$$

is well defined and it is a *conditional expectation*, that is, $^{K}(f_1 * f * f_2)^{K} = f_1 * {}^{K}f^{K} * f_2$ for all $f_1, f_2 \in {}^{K}L(G)^{K}$ and $f \in L(G)$.

(4) Show that $(f_1 * f_2)^* = f_2^* * f_1^*$ for all $f_1, f_2 \in L(G)$.

Definition 1.2.50 Suppose that G acts transitively on a set X. The *permutation representation* $(\lambda, L(X))$ is the G-representation defined by setting

$$[\lambda(g)f](x) = f(g^{-1}x) \quad \text{for all } f \in L(X), g \in G, x \in X.$$

Exercise 1.2.51 Show that the permutation representation $(\lambda, L(X))$ is unitary.

Proposition 1.2.52 *Suppose that G acts transitively on a set X. Let $x_0 \in X$ and set $K = \mathrm{Stab}_G(x_0)$. Then $\mathrm{End}_G(L(X))$ and ${}^K L(G)^K$ are isomorphic as algebras.*

Proof Given a linear map $T\colon L(X) \to L(X)$, there exists a matrix $(r(x,y))_{x,y\in X}$ such that

$$[Tf](x) = \sum_{y\in X} r(x,y)f(y) \quad \text{for all } f \in L(X) \text{ and } x \in X. \tag{1.2}$$

We have that $T \in \mathrm{End}_G(L(X))$ if and only if $r(gx,gy) = r(x,y)$ for all $g \in G$ and $x,y \in X$, and this is in turn equivalent to saying that r is constant on the G-orbits on $X \times X$. Define $\psi\colon X \to \mathbb{C}$ by setting

$$\psi(x) = r(x,x_0) \quad \text{for all } x \in X. \tag{1.3}$$

Note that ψ is K-invariant: $\psi(kx) = r(kx,x_0) = r(kx,kx_0) = r(x,x_0) = \psi(x)$, so that $\widetilde{\psi} \in {}^K L(G)^K$. Moreover (1.2) becomes

$$\begin{aligned}[\widetilde{Tf}](g) = [Tf](gx_0) &= \frac{1}{|K|}\sum_{h\in G} r(gx_0,hx_0)f(hx_0) \\ &= \frac{1}{|K|}\sum_{h\in G} f(hx_0)r(h^{-1}gx_0,x_0) = \frac{1}{|K|}[\widetilde{f} * \widetilde{\psi}](g),\end{aligned} \tag{1.4}$$

and we say that $\frac{1}{|K|}\widetilde{\psi} \in {}^K L(G)^K$ is the *kernel* of T.

However, if $T_1, T_2 \in \mathrm{End}_G(L(X))$ and $\widetilde{\psi}_1, \widetilde{\psi}_2$ are the associated kernels, we have that the kernel of $T_1 \circ T_2$ is $\frac{1}{|K|^2}\widetilde{\psi}_2 * \widetilde{\psi}_1$. Thus, if we set $f^\sharp(g) = f(g^{-1})$ for all $f \in L(G)$ and $g \in G$, we deduce that the desired isomorphism is given by $T \mapsto \frac{1}{|K|}(\widetilde{\psi})^\sharp$. □

Definition 1.2.53 (Gelfand pair) (G,K) is a *Gelfand pair* if the algebra ${}^K L(G)^K$ is commutative.

Exercise 1.2.54 (Symmetric Gelfand pairs) Let G be a finite group and let $K \leq G$ be a subgroup. Suppose that

$$g^{-1} \in KgK \quad \text{for all } g \in G. \tag{1.5}$$

Show that (G,K) is a Gelfand pair. We then say that (G,K) is a *symmetric* Gelfand pair.

More generally, we have:

Exercise 1.2.55 Suppose that there exists $\tau \in \mathrm{Aut}(G)$ such that

$$g^{-1} \in K\tau(g)K \quad \text{for all } g \in G. \tag{1.6}$$

Show that (G,K) is a Gelfand pair. We then say that (G,K) is a *weakly symmetric* Gelfand pair.

Exercise 1.2.56 Let $\widetilde{G} = \{(g,g) : g \in G\}$ denote the diagonal subgroup of $G \times G$.

(1) Show that $(G \times G, \widetilde{G})$ is a Gelfand pair. (See [62] for a more general construction.)
(2) Show that the Gelfand pair $(G \times G, \widetilde{G})$ is symmetric if and only if G is *ambivalent*, that is, every element $g \in G$ is conjugate in G to its inverse g^{-1}.

Exercise 1.2.57 Suppose that G acts transitively on a set X; let $x_0 \in X$, set $K = \mathrm{Stab}_G(x_0)$, and consider the diagonal action of G on $X \times X$. Show that (G,K) is a symmetric Gelfand pair if and only if the G-orbits on $X \times X$ are symmetric, i.e. $G(x,y) = G(y,x)$ for all $x,y \in X$.

Exercise 1.2.58 Let G act on a metric space (X,d) and suppose that the action is *two-point homogeneous* (or *distance transitive*) i.e., $G(x_1,y_1) = G(x_2,y_2)$ if $d(x_1,y_1) = d(x_2,y_2)$. Show that (G,K) is a symmetric Gelfand pair.

Definition 1.2.59 A G-representation (ρ,V) is *multiplicity-free* if it does not contain two equivalent irreducible representations, in formulæ,

$$\rho = \oplus_{\theta \in \widehat{G}} m_\theta^\rho \theta \Rightarrow m_\theta^\rho \leq 1 \text{ for all } \theta \in \widehat{G}.$$

Theorem 1.2.60 *The following conditions are equivalent:*

(1) (G,K) *is a Gelfand pair;*
(2) $\mathrm{End}_G(L(X))$ *is commutative;*
(3) $(\lambda, L(X))$ *is multiplicity-free.*

Proof The equivalence between (1) and (2) follows from Proposition 1.2.52.

Suppose that (3) holds, i.e.

$$L(X) = \oplus_{i=0}^N V_i$$

with V_i irreducible and $V_i \not\sim V_j$ if $i \neq j$.

If $T \in \mathrm{End}_G(L(X))$, then $T_i = T|_{V_i}$ is either trivial ($T_i = 0$) or injective (since

https://doi.org/10.1017/9781009465939.002 Published online by Cambridge University Press

$\ker T_i$ is a G-invariant subspace of V_i). In the latter case $\operatorname{ran} T_i \le L(X)$ is G-invariant and isomorphic to V_i. Thus $\operatorname{ran}(T_i) \cap V_j \le V_j$ is either 0 or V_j. This holds only if $j = i$. Therefore, by Schur's lemma there exists $\lambda_i \in \mathbb{C}$ such that $T_i = \lambda_i P_{V_i}$ (with P_{V_i} the orthogonal projection on V_i) and $T = \sum_{i=0}^N \lambda_i P_{V_i}$. If $S \in \operatorname{End}_G(L(X))$ is another intertwiner, then $S = \sum_{i=0}^N \mu_i P_{V_i}$ and therefore we have $ST = \sum_{i=0}^N \mu_i \lambda_i P_{V_i} = TS$, showing the commutativity of $\operatorname{End}_G(L(X))$.

Vice versa, suppose that (2) holds. If $L(X)$ is not multiplicity-free, then $L(X) = V \oplus W \oplus U$ with $V \sim W$ irreducible. Let $R \in \operatorname{Hom}_G(V,W)$ be an isomorphism. Consider the linear operators $S,T : L(X) \to L(X)$ defined by setting

$$\begin{aligned} S(v+w+u) &= R^{-1}w \\ T(v+w+u) &= Rv \end{aligned}$$

for all $v \in V$, $w \in W$, $u \in U$. We have that $T,S \in \operatorname{End}_G(L(X))$: indeed, for $v \in V$, $w \in W$, $u \in U$, and $g \in G$,

$$\begin{aligned} T\lambda(g)(v+w+u) &= T(\lambda(g)v + \lambda(g)w + \lambda(g)u) \\ &= R\lambda(g)v \\ &= \lambda(g)Rv \\ &= \lambda(g)T(v+w+u). \end{aligned}$$

The proof for S is completely analogous. Observe that $STv = v$, while $TSv = 0$, thus showing that $\operatorname{End}_G(L(X))$ is not commutative. $\square$

With the notation of the above proof, we have the following:

Corollary 1.2.61 *The map* $\operatorname{End}_G(L(X)) \ni T \mapsto (\lambda_0, \lambda_1, \ldots, \lambda_N) \in \mathbb{C}^{N+1}$ *is an algebra isomorphism.* $\square$

From the above results we deduce :

$$\begin{aligned} N+1 &= |\{\text{irreducible sub-representations in } L(X)\}| \\ &= \dim \operatorname{End}_G(L(X)) \\ &= \dim {}^K L(G)^K \\ &= |K \backslash G / K| \\ &= |\{K\text{-orbits on } X\}|. \end{aligned}$$

1.2.3 Spherical functions

In this section we suppose that (G,K) is a Gelfand pair.

Definition 1.2.62 (Spherical function) A function $\phi \in {}^K L(G)^K$ is *spherical* if

https://doi.org/10.1017/9781009465939.002 Published online by Cambridge University Press

- for every $f \in {}^K L(G)^K$ there exists $\lambda_f \in \mathbb{C}$ such that $f * \phi = \lambda_f \phi$;
- $\phi(1_G) = 1$.

Note that if ϕ is a spherical function and $f \in {}^K L(G)^K$, then $\lambda_f = [f * \phi](1_G)$.

Lemma 1.2.63 *Let ϕ be a spherical function. Define $\Phi \colon L(G) \to \mathbb{C}$ by setting*

$$\Phi(f) = \sum_{g \in G} f(g)\phi(g^{-1}) \tag{1.7}$$

for all $f \in L(G)$. Then Φ is a linear multiplicative functional on ${}^K L(G)^K$, that is, $\Phi(f_1 * f_2) = \Phi(f_1)\Phi(f_2)$ for all $f_1, f_2 \in {}^K L(G)^K$. Vice versa, every nontrivial multiplicative linear functional on ${}^K L(G)^K$ is determined by a unique spherical function.

Proof We leave it to the reader to check that Φ is a multiplicative linear functional.

Vice versa, suppose that Φ is a multiplicative linear functional on ${}^K L(G)^K$. Then we can extend Φ to a linear functional $\widetilde{\Phi}$ on $L(G)$ by setting $\widetilde{\Phi}(f) = \Phi({}^K f^K)$ for all $f \in L(G)$. By Riesz' representation theorem there exists $\psi \in L(G)$ such that $\widetilde{\Phi}(f) = \sum_{g \in G} f(g)\psi(g^{-1})$. We leave it to the reader to check that the function $\phi := {}^K \psi^K \in {}^K L(G)^K$ is spherical and satisfies (1.7) for all $f \in {}^K L(G)^K$. $\square$

Proposition 1.2.64 (Basic properties of spherical functions) *Let ϕ and ψ be two distinct spherical functions. Then:*

- $\phi(g^{-1}) = \overline{\phi(g)}$ *for all $g \in G$;*
- $\phi * \psi = 0$*;*
- $\langle \lambda(g_1)\phi, \lambda(g_2)\psi \rangle_{L(G)} = 0$ *for all $g_1, g_2 \in G$ (in particular $\phi \perp \psi$).*

Proof We leave it to the reader. $\square$

Theorem 1.2.65

$$|\{\textit{spherical functions}\}| = |K \backslash G / K| = \dim {}^K L(G)^K.$$

In particular, the spherical functions constitute an orthogonal basis for the space of all bi-K-invariant functions on G.

Proof By Proposition 1.2.52 and Corollary 1.2.61, the algebras ${}^K L(G)^K$ and $\mathbb{C}^{N+1}$ are isomorphic. The statement follows by observing that the only multiplicative linear functionals on $\mathbb{C}^{N+1}$ are the maps

$$\begin{array}{cccc} \Phi_j\colon & \mathbb{C}^{N+1} & \to & \mathbb{C} \\ & (\alpha_0, \alpha_1, \ldots, \alpha_N) & \mapsto & \alpha_j \end{array}$$

$j = 0, 1, \ldots, N$. $\square$

https://doi.org/10.1017/9781009465939.002 Published online by Cambridge University Press

For $f \in L(G)^K$ define $\check{f} \in L(X)$ by setting $\check{f}(gx_0) = f(g)$ for all $g \in G$ (as usual, $x_0 = K \in G/K$; equivalently, $x_0 \in X$ and $K = \mathrm{Stab}_G(x_0)$).

Theorem 1.2.66 *Let $\phi_0, \phi_1, \ldots, \phi_N \in {}^K L(G)^K$ be the spherical functions. Set*

$$V_i = \mathrm{span}\{\lambda(g)\check{\phi}_i : g \in G\} \leq L(X)$$

for $i = 0, 1, \ldots, N$. Then

$$L(X) = \bigoplus_{i=0}^{N} V_i$$

is the decomposition of the permutation representation into irreducible sub-representations.

Proof Each V_i is G-invariant and, being cyclic (that is, G-generated by a single vector), is irreducible. Moreover $V_i \perp V_j$ if $i \neq j$ (cf. Proposition 1.2.64). Since there are exactly $N+1$ irreducible components of $L(X)$, we conclude that the V_i's exhaust all of $L(X)$. □

Definition 1.2.67 $(\lambda|_{V_i}, V_i)$ is called the *spherical representation* associated with ϕ_i.

We always choose $\phi_0 \equiv 1$ so that V_0 is the trival representation.

Exercise 1.2.68 The spherical functions of the Gelfand pair $(G \times G, \widetilde{G})$ (cf. Exercise 1.2.56) are the normalized characters of G, namely, the bi-$\widetilde{G}$-invariant functions φ_σ, $\sigma \in \widehat{G}$, defined by

$$\varphi_\sigma(g,h) = \frac{1}{d_\sigma}\chi^\sigma(g^{-1}h)$$

for all $g, h \in G$.

Let (ρ, V) be a G-representation. We denote by

$$V^{\rho,K} = \{v \in V : \rho(k)v = v, \text{ for all } k \in K\}$$

the subspace of K-*invariant* vectors. If the representation ρ is clear from the context we will simply write V^K for $V^{\rho,K}$. However, note that $L(G)^K = L(G)^{\rho_G,K}$ while ${}^K L(G) = L(G)^{\lambda_G,K}$ (cf. Example 1.2.14) and we write ${}^K L(X)$ for $L(X)^{\lambda,K}$ (cf. Definition 1.2.50).

For the proof of Theorem 1.2.71 we need a couple of classical results from the theory of group actions, namely the so-called *Burnside lemma* and the *Wielandt lemma*. The first result is not due to Burnside himself, who merely quotes it in his book [10], attributing it instead to Frobenius, although it was already known to Cauchy (cf. [54, 72]). For a proof we refer to [6] (see also [15, Lemma 3.11.1]).

Exercise 1.2.69 (Burnside's lemma) Let G be a finite group acting (not necessarily transitively) on a finite set Ω. Denote by $(\lambda, L(\Omega))$ the *permutation representation*, defined by setting $[\lambda(g)f](\omega) = f(g^{-1}\omega)$ for all $g \in G$, $f \in L(\Omega)$, and $\omega \in \Omega$. Denote by $\chi = \chi^\lambda$ the associated character. Show that

$$\frac{1}{|G|}\sum_{g\in G}\chi(g) = \frac{1}{|G|}\sum_{\omega\in\Omega}|\operatorname{Stab}_G(\omega)| = \text{ number of } G\text{-orbits in } \Omega.$$

The result in the next exercise was surely known to Schur and, possibly, even to Frobenius. A standard reference is the book by Helmut Wielandt [70] (see also [15, Theorem 3.13.3]).

Exercise 1.2.70 (Wielandt's lemma) Let $K \leq G$ be finite groups and set $X := G/K$. Let $L(X) = \bigoplus_{i=0}^N m_i V_i$ be a decomposition into irreducible G-subrepresentations of the associated permutation representation, where m_i denotes the multiplicity of V_i. Then

$$\sum_{i=0}^N m_i^2 = \text{ number of } G\text{-orbits on } X\times X \;=\; \text{number of } K\text{-orbits on } X. \qquad (1.8)$$

Theorem 1.2.71 *(G,K) is a Gelfand pair if and only if $\dim V^{\rho,K} \leq 1$ for all $(\rho, V) \in \widehat{G}$. If this is the case, then $\dim V^{\rho,K} = 1$ if and only if (ρ, V) is equivalent to a spherical representation.*

Proof Let $(\rho, V) \in \widehat{G}$ with $\dim V^{\rho,K} \geq 1$. Pick $u_0 \in V^{\rho,K}$ and define $T: V \to L(X) = L(G/K)$ by setting $[Tv](gK) = (\langle v, \rho(g)u_0\rangle_V)\check{}$. Now $T \in \operatorname{Hom}_G(V, L(X))$, and by Schur's lemma we deduce that $V \sim V_{\bar{\imath}}$ for some $0 \leq \bar{\imath} \leq N$. Since $L(X) = \oplus_{i=0}^N V_i$,

$$N+1 = \dim L(X)^{\lambda,K} = (\dim^K L(G)^K),$$

and $L(X)^{\lambda,K} = \oplus_{i=0}^N V_i^{\lambda,K}$, we deduce that $\dim V_i^{\lambda,K} \leq 1$ for all $i = 0,1,\ldots,N$. This in turn implies that $\dim V^{\rho,K} = \dim V_{\bar{\imath}}^{\lambda,K} \leq 1$.

Vice versa, suppose that $\dim V^{\rho,K} \leq 1$ for all $(\rho, V) \in \widehat{G}$. Let $L(X) = \oplus_{i=0}^H m_i W_i$ be the decomposition of the permutation representation into irreducible components. If $N+1$ is the number of K-orbits on X we have (keeping in mind (1.8))

$$\sum_{i=0}^H m_i^2 = N+1 = \sum_{i=0}^H m_i \dim W_i^{\lambda,K} \leq \sum_{i=0}^H m_i. \qquad (1.9)$$

This forces $m_i = 1$ for all $i = 0,1,\ldots,H$ and $H = N$. $\square$

https://doi.org/10.1017/9781009465939.002 Published online by Cambridge University Press

1.2.4 Harmonic analysis of finite Gelfand pairs

Let (G,K) be a finite Gelfand pair and denote by $\phi_0 = 1, \phi_1, \ldots, \phi_N \in {}^K L(G)^K$ the associated spherical functions.

Definition 1.2.72 The linear map $\mathscr{F} : {}^K L(X) \to \mathbb{C}^{N+1}$ defined by setting

$$[\mathscr{F} f](i) = \langle f, \check{\phi}_i \rangle_{L(X)} = \sum_{x \in X} f(x) \overline{\check{\phi}_i(x)}$$

for all $f \in {}^K L(X)$ and $i = 0, 1, \ldots, N$, is called the *spherical Fourier transform* associated with the Gelfand pair (G,K).

Exercise 1.2.73 (Inversion formula) Let $f \in {}^K L(X)$. Show that

$$f(x) = \frac{1}{|X|} \sum_{i=0}^{N} d_i [\mathscr{F} f](i) \check{\phi}_i(x), \tag{1.10}$$

where, as usual, $d_i = \dim(V_i)$ is the dimension of the ith spherical representation.

Proposition 1.2.74 *Let $T \in \mathrm{End}_G(L(X))$. Then, for all $i = 0, 1, \ldots, N$,*

$$T|_{V_i} = \lambda_i I_{V_i},$$

where $\lambda_i = [\mathscr{F}\psi](i)$ and $\psi \in {}^K L(X)$ is as in (1.2) *and* (1.3).

Proof Let $x_0 \in X$ be the point stabilized by K. Then, for all $g \in G$ we have

$$\begin{aligned}
[T\check{\phi}_i](gx_0) &= \frac{1}{|K|}[\phi_i * \widetilde{\psi}](g) \\
&= \frac{1}{|K|}[\phi_i * \widetilde{\psi}](1_G)\phi_i(g) \\
&= \frac{1}{|K|}\left(\sum_{h \in G} \phi_i(h^{-1})\widetilde{\psi}(h)\right)\phi_i(g) \\
&= \frac{1}{|K|}\langle \widetilde{\psi}, \phi_i \rangle_{L(G)} \phi_i(g) \\
&= \langle \psi, \check{\phi}_i \rangle_{L(X)} \check{\phi}_i(gx_0) \\
&= [\mathscr{F}\psi](i)\check{\phi}_i(gx_0).
\end{aligned}$$

As T is an intertwiner, we deduce that $Tv = \lambda_i v$ for all $v \in V_i$, where $\lambda_i = [\mathscr{F}\psi](i)$. $\square$

Remark 1.2.75 Let $\Omega \subseteq X$ be a K-orbit and denote by $1_\Omega \in L(X)$ its characteristic function. Then

$$[\mathscr{F} 1_\Omega](i) = |\Omega| \overline{\check{\phi}_i(x)}$$

https://doi.org/10.1017/9781009465939.002 Published online by Cambridge University Press

where $x \in \Omega$ is arbitrary (spherical functions are constant on K-orbits).

Definition 1.2.76 (Convolution in $L(X)$) Let G be a finite group acting transitively on a finite set X. Let $x_0 \in X$ and set $K := \mathrm{Stab}_G(x_0)$. The *convolution* of two functions $f_1, f_2 \in L(X)$ is the function $f_1 * f_2 \in L(X)$ defined by setting

$$f_1 * f_2 := \frac{1}{|K|}(\widetilde{f_1} * \widetilde{f_2})\check{}.$$

Given $f \in L(X)$ we write $f^{*1} := f$ and, for $n \geq 2$, we recursively set $f^{*n} := f * (f^{*(n-1)})$.

Exercise 1.2.77 Let $f_1, f_2 \in {}^K L(X)$. Show that $f_1 * f_2 \in {}^K L(X)$ and

$$\mathscr{F}(f_1 * f_2) = \mathscr{F}(f_1)\mathscr{F}(f_2). \tag{1.11}$$

Exercise 1.2.78 Show that the orthogonal projection $P_i \colon L(X) \to V_i$ is given by

$$[P_i f](gx_0) = \frac{d_i}{|X|}\langle f, \lambda(g)\check{\phi}_i\rangle_{L(X)}$$

for all $f \in L(X)$.

1.3 Laplace operators and spectra of random walks on finite graphs

In this section we present some elementary theory of finite regular simple graphs and the spectral theory of their associated adjacency (resp. Markov, resp. Laplace) matrices. A particular emphasis is given for a particular, yet significant, subclass of such graphs, namely that of distance-regular graphs. We refer to our monographs [15, 19] for other related aspects of finite graph theory.

1.3.1 Finite graphs and their spectra

Definition 1.3.1 (Finite graph) A *finite graph* is a pair $\mathscr{G} = (X, E)$, where X is a finite set of *vertices* and E is a subset of $\{\{x,y\} : x,y \in X\}$, called the set of *edges*. An edge of the form $e = \{x\} \in E$ is called a *loop* at x.

Let $\mathscr{G} = (X,E)$ be a finite graph. Given $e = \{x,y\} \in E$, we say that the vertices x and y are *adjacent* (or *neighbours*) and we write $x \sim y$. Given $x \in X$, we denote by $\deg(x) := |\{y \in X : x \sim y\}|$ the number of adjacent vertices (including x itself if there is a loop at x). If $\deg(x) = \deg(y) =: k$ for all $x, y \in X$, one says that $\mathscr{G}$ is *regular* of *degree* k.

Given a subset $Y \subset X$ of vertices, the *subgraph induced* by Y is the graph $\mathscr{G}_Y = (Y, E_Y)$ where $E_Y := \{e = \{x,y\} \in E : x,y \in Y\}$.

A *path* in $\mathscr{G}$ is a sequence $\pi = (x_0, x_1, \ldots, x_n)$ of vertices $x_i \in X$ such that $x_i \sim x_{i+1}$ for all $i = 0, 1, \ldots, n-1$. The vertices x_0 and x_n are termed the *initial* and *terminal* vertices of π, and one says that π connects them. The integer n is called the *length* of the path π, denoted $\ell(\pi)$.

We introduce an equivalence relation $\approx$ on X by declaring that $x \approx y$ if there exists a path $\pi = \pi(x,y)$ connecting them. The subgraph induced by an $\approx$ equivalence class is called a *connected component* of $\mathscr{G}$. If there exists a unique such connected component, one says that $\mathscr{G}$ is *connected*.

If $\mathscr{G}$ is connected, given two vertices x and y, the nonnegative integer $d(x,y) := \min_\pi \ell(\pi)$, where π ranges among all paths $\pi = \pi(x,y)$, is called the *distance* of x and y. The nonnegative integer $\mathrm{diam}(X) := \max\{d(x,y) : x,y \in X\}$ is called the *diameter* of the connected graph $\mathscr{G} = (X,E)$.

This way, our finite graphs are simple, i.e., with no multiple edges, and undirected.

Exercise 1.3.2 Let $\mathscr{G} = (X,E)$ be a finite graph. Show that the map $d \colon X \times X \to [0, +\infty)$ is a distance function.

Definition 1.3.3 (Adjacency and Markov matrices and Laplacian) Let $\mathscr{G} = (X,E)$ be a finite graph. The matrix $A = (A(x,y))_{x,y \in X}$ where

$$A(x,y) := \begin{cases} 1 & \text{if } x \sim y, \\ 0 & \text{otherwise,} \end{cases}$$

for all $x, y \in X$, is called the *adjacency matrix* of $\mathscr{G}$.

If $\mathscr{G}$ is regular of degree k, the matrices

$$M := \frac{1}{k} A \ \text{ and } L := I - M \equiv I - \frac{1}{k} A, \tag{1.12}$$

https://doi.org/10.1017/9781009465939.002 Published online by Cambridge University Press

where $I = (\delta_{x,y})_{x,y \in X}$ is the identity matrix, are called the *Markov matrix* and the *discrete Laplacian* on $\mathscr{G}$, respectively.

Note that the Laplacian can be defined for arbitrary graphs, not necessarily regular: see Definition 3.2.11.

In the following we shall limit ourselves to the case where $\mathscr{G}$ is k-regular.

Recall that the spectrum $\sigma(T)$ of $T \in \mathrm{End}(L(X))$ is the set of all eigenvalues of T:

$$\sigma(T) := \{\lambda \in \mathbb{C} : T - \lambda I \text{ is not invertible in } \mathrm{End}(L(X))\}.$$

If T is symmetric, then the spectrum is real: $\sigma(T) =: \{\lambda_0, \lambda_1, \ldots, \lambda_m\} \subseteq \mathbb{R}$, and, denoting by V_i the T-eigenspace associated with λ_i, $i = 0, 1, \ldots, m$, we have the decomposition

$$L(X) = \bigoplus_{i=0}^{m} V_i. \tag{1.13}$$

In our setting, we have $\sigma(A) \subseteq [-k,k]$, $\sigma(M) \subseteq [-1,1]$, and $\sigma(L) \subseteq [0,2]$. Moreover, given the simple expressions (1.12) relating A, M, and L, the corresponding spectra are set-theoretically related by the expressions $\sigma(M) = \frac{1}{k}\sigma(A)$ and $\sigma(L) = 1 - \sigma(M) = 1 - \frac{1}{k}\sigma(A)$, and the corresponding eigenspaces coincide (we leave it as an exercise to check the details). For this reason, we limit ourselves to the analysis of the Markov matrix M.

We first note that $\lambda_0 := 1$ is an eigenvalue of M: indeed, any constant function $f \in L(X)$ (or, more generally, any function $f \in L(X)$ which is constant on each connected component of $\mathscr{G}$) is an M-eigenvector corresponding to the eigenvalue 1, that is, $Mf = f$. More precisely, we have the following:

Proposition 1.3.4 *Let $\mathscr{G} = (X,E)$ be a k-regular finite graph. Let $V_0 \leq L(X)$ denote the M-eigenspace corresponding to the eigenvalue $\lambda_0 = 1$. Then* $\dim(V_0)$ *equals the number of connected components of $\mathscr{G}$.*

Proof Let $\mathscr{G}_i = (X_i, E_i)$, $i = 1, 2, \ldots, n$, be the connected components of $\mathscr{G}$. It is obvious that if f is constant on each $\mathscr{G}_i$, then $Mf = f$. As the characteristic functions $\chi_{X_i} \in L(X)$ are linearly independent, this shows that $\dim(V_0) \geq n$. Conversely, suppose that $Mf = f$ with $f \in L(X)$ non-identically zero and real valued. Fix $i \in \{1, 2, \ldots, n\}$ and denote by $x_i \in X_i$ a maximum point for $|f|$ in X_i, i.e. $|f(x_i)| \geq |f(y)|$ for all $y \in X_i$; we may suppose, up to passing to $-f$, that $f(x_i) \geq 0$. Then $f(x_i) = \sum_{y \in X_i} m(x_i,y) f(y)$ and as $\sum_{y \in X_i} m(x_i,y) = 1$ we have $\sum_{y \in X_i} m(x_i,y)[f(x_i) - f(y)] = 0$. Since $m(x_i,y) \geq 0$ and $f(x_i) \geq f(y)$ for all $y \in X_i$, we deduce that $f(y) = f(x_i)$ for all $y \sim x_i$. Let now $z \in X_i$; then, by definition, there exists a path $p = (x_i, x_i', \ldots, x_i'' = z)$ connecting x_0 to z. In

https://doi.org/10.1017/9781009465939.002 Published online by Cambridge University Press

the previous step we have established that $f(x_i') = f(x_i) \geq f(y)$ for all $y \in X_i$ so that we can iterate the same argument to show that $f(x_i) = f(x_i') = \cdots = f(x_i'') = f(z)$, i.e., f is constant in X_i. This shows that V_0 is spanned by the χ_{X_i}s. We deduce that $\dim(V_0) = n$. □

Definition 1.3.5 A graph $\mathscr{G} = (X,E)$ is *bipartite* if there exists a nontrivial partition $X = X_0 \sqcup X_1$ of the set of vertices such that every edge joins a vertex in X_0 with a vertex in X_1; that is, $E \subseteq \{\{x_0,x_1\} : x_0 \in X_0, x_1 \in X_1\}$.

Note that a bipartite graph has no loops and that, if $\mathscr{G}$ is connected, then the partition of the set of vertices is unique.

Example 1.3.6 Figure 1.1 shows the bipartite graph $\mathscr{G} = (X,E)$ with vertex set $X = X_0 \sqcup X_1$, where $X_0 = \{x,y\}$ and $X_1 = \{u,v,z\}$, and edge set $E = \{\{x,u\},\{x,v\},\{y,v\},\{y,z\}\}$.

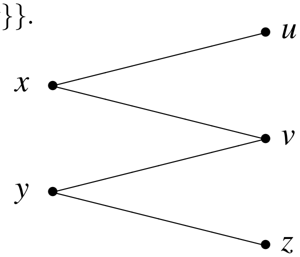

Figure 1.1 A bipartite graph

Exercise 1.3.7 Let $\mathscr{G} = (X,E)$ be a connected graph. Show that the following conditions are equivalent:

(1) $\mathscr{G}$ is bipartite;
(2) $\mathscr{G}$ is *bicolorable*, i.e., there exists a map $\phi\colon X \to \{0,1\}$ such that $x \sim y$ implies $\phi(x) \neq \phi(y)$ for all $x,y \in X$;
(3) every closed path in $\mathscr{G}$ has even length;
(4) there exists $x_0 \in X$ such that every closed path containing x_0 has even length;
(5) given $x,y \in X$, then for all paths p connecting x and y one has $|p| \equiv d(x,y) \mod 2$, that is $|p| - d(x,y)$ is even.

Proposition 1.3.8 *Let $\mathscr{G} = (X,E)$ be a k-regular connected graph and denote by M the associated Markov matrix. Then the following conditions are equivalent:*

(1) *$\mathscr{G}$ is bipartite;*
(2) *the spectrum $\sigma(M)$ is symmetric: $\lambda \in \sigma(M)$ if and only if $-\lambda \in \sigma(M)$;*
(3) $-1 \in \sigma(M)$.

https://doi.org/10.1017/9781009465939.002 Published online by Cambridge University Press

Proof Suppose that $\mathscr{G}$ is bipartite with $X = X_0 \sqcup X_1$ and that $Mf = \lambda f$. Define $\widetilde{f} \in L(X)$ by setting $\widetilde{f}(x) := (-1)^j f(x)$ for all $x \in X_j$, $j = 0, 1$. Then, for $x \in X_j$ we have:

$$\begin{aligned}
[M\widetilde{f}](x) &= \sum_{y:y\sim x} m(x,y)\widetilde{f}(y) \\
&= (-1)^{j+1} \sum_{y:y\sim x} m(x,y) f(y) \\
&= (-1)^{j+1} \lambda f(x) \\
&= -\lambda \widetilde{f}(x).
\end{aligned}$$

We have shown that if λ is an eigenvalue for f, then $-\lambda$ is an eigenvalue for $\widetilde{f}$; this gives the implication (1) $\Longrightarrow$ (2).

Since we always have $1 \in \sigma(M)$ (cf. Proposition 1.3.4), the implication (2) $\Longrightarrow$ (3) is obvious.

Finally suppose that $Mf = -f$ with $f \in L(X)$ nontrivial and real valued. Denote by $x_0 \in X$ a point of maximum for $|f|$; then, up to switching f to $-f$, we may suppose that $f(x_0) > 0$. We then have that $-f(x_0) = \sum_{y:y\sim x_0} m(x_0,y) f(y)$ implies $\sum_{y:y\sim x_0} m(x_0,y)[f(x_0) + f(y)] = 0$. Since $f(x_0) + f(y) \geq 0$ we deduce $f(y) = -f(x_0)$ for all $y \sim x_0$. Set $X_j := \{y \in X : f(y) = (-1)^j f(x_0)\}$ for $j = 0, 1$. We claim that $X = X_0 \sqcup X_1$: indeed $\mathscr{G}$ is connected and if $p = (x_0, x_1, \ldots, x_m)$ is a path, then $f(x_j) = (-1)^j f(x_0)$. Finally, if $y \sim z$ we clearly have $f(y) = -f(z)$ so that $\mathscr{G}$ is bicolorable, that is, it is bipartite. □

Definition 1.3.9 (Distance-regular graphs) (See also Definition 2.5.4.) A finite graph $\mathscr{G} = (X, E)$ with no loops is called *distance-regular* if there exist two sequences of constants, called the *$\mathscr{G}$-parameters*, $b_0, b_1, \ldots, b_N$ and $c_0, c_1, \ldots, c_N$, where $N = \mathrm{diam}(\mathscr{G})$, such that, for any pair of vertices $x, y \in X$ with $d(x,y) = i$ one has

$$\begin{aligned}
|\{z \in X : d(x,z) = 1, d(y,z) = i+1\}| &= b_i \\
|\{z \in X : d(x,z) = 1, d(y,z) = i-1\}| &= c_i
\end{aligned}$$

for all $i = 0, 1, \ldots, N$. In other words, if $d(x,y) = i$, then x has b_i neighbors at distance $i+1$ from y and c_i neighbors at distance $i-1$ from y. In particular, taking $x = y$ we get $b_0 = |\{z \in X : d(x,z) = 1\}|$, for all $x \in X$, that is, $\mathscr{G}$ is regular of degree b_0.

Exercise 1.3.10 Let $\mathscr{G}$ be a distance-regular graph. Show that the following hold:

(1) $b_N = 0 = c_0$;
(2) $c_1 = 1$;

(3) for $x,y \in X$ with $d(x,y) = i$ one has $|\{z \in X : d(x,z) = 1, d(y,z) = i\}| = b_0 - b_i - c_i$;
(4) for any $x \in X$, the cardinality $k_i := |\{y \in X : d(x,y) = i\}|$ of the sphere of radius i centered at x is given by $k_i = b_0 b_1 \cdots b_{i-1}/c_2 c_3 \cdots c_i$, for $i = 2,3,\ldots,N$.

Let $\mathscr{G} = (X,E)$ be a distance-regular graph. For $j = 0,1,\ldots,N$, we define the matrix $A_j = (A_j(x,y))_{x,y \in X}$ by setting

$$A_j(x,y) := \begin{cases} 1 & \text{if } d(x,y) = j \\ 0 & \text{otherwise.} \end{cases} \tag{1.14}$$

Note that $A_0 = I$ and A_1 is the adjacency matrix of $\mathscr{G}$. We denote by $\mathscr{A}$ the subalgebra of $\mathrm{End}(L(X))$ generated by $A_0, A_1, \ldots, A_N$. It is called the *Bose–Mesner algebra* associated with $\mathscr{G}$ (see [3, 4] and [2]).

Proposition 1.3.11 *Let $\mathscr{G} = (X,E)$ be a distance-regular graph as in Definition 1.3.9. Then the following hold.*

(1) *For $j = 0,1,\ldots,N$,*

$$A_j A_1 = b_{j-1} A_{j-1} + (b_0 - b_j - c_j) A_j + c_{j+1} A_{j+1}, \tag{1.15}$$

where $A_{N+1} = 0$.

(2) *For $j = 0,1,\ldots,N$ there exists a real polynomial p_j of degree j such that*

$$A_j = p_j(A_1). \tag{1.16}$$

In particular, $\mathscr{A} = \{p(A_1) : p \text{ polynomial over } \mathbb{C}\}$ is commutative, and its dimension is $N+1$. In fact, $A_0, A_1, \ldots, A_N$ constitute a vector space basis for $\mathscr{A}$.

(3) *Let*

$$L(X) = \oplus_{i=0}^{n} V_i \tag{1.17}$$

denote the decomposition into distinct eigenspaces of A_1, with V_0 the one-dimensional space of constant functions. Then $n = N$ and each V_i is invariant for all operators $A \in \mathscr{A}$. Moreover, if V_0 is the subspace of constant functions, the eigenvalue λ_0 of A_1 corresponding to V_0 is equal to the degree of X, that is, $\lambda_0 = b_0$.

(4) *Denote by E_i the orthogonal projection onto V_i and let λ_i denote the eigenvalue of A_1 corresponding to V_i. Then,*

$$A_j = \sum_{i=0}^{N} p_j(\lambda_i) E_i, \tag{1.18}$$

where p_j is the polynomial in (1.16). Similarly, the projection $E_i := q_i(A_1)$ for some polynomial q_i.

Proof (1) For $f \in L(X)$ and $y \in X$ one clearly has

$$\begin{aligned}
(A_jA_1f)(y) &= \sum_{\substack{z\in X:\\ d(z,y)=j}} (A_1f)(z) = \\
&= \sum_{\substack{z\in X:\\ d(z,y)=j}} \sum_{\substack{x\in X:\\ d(x,z)=1}} f(x) = \\
&= \sum_{\substack{z\in X:\\ d(z,y)=j}} \left(\sum_{\substack{x\in X:\\ d(x,z)=1\\ d(x,y)=j-1}} f(x) + \sum_{\substack{x\in X:\\ d(x,z)=1\\ d(x,y)=j}} f(x) + \sum_{\substack{x\in X:\\ d(x,z)=1\\ d(x,y)=j+1}} f(x) \right) = \\
&= b_{j-1} \sum_{\substack{x\in X:\\ d(x,y)=j-1}} f(x) + \\
&\qquad + (b_0 - b_j - c_j) \sum_{\substack{x\in X:\\ d(x,y)=j}} f(x) + \\
&\qquad\qquad + c_{j+1} \sum_{\substack{x\in X:\\ d(x,y)=j+1}} f(x) = \\
&= b_{j-1}\left(A_{j-1}f\right)(y) + (b_0 - b_j - c_j)(A_jf)(y) + c_{j+1}\left(A_{j+1}f\right)(y)
\end{aligned}$$

because for any x with $d(x,y) = j-1$ there exist b_{j-1} elements $z \in X$ such that $d(x,z) = 1$ and $d(z,y) = j$, and therefore $f(x)$ appears b_{j-1} times in the above sums. A similar argument holds for $d(x,y) = j$ or $j+1$ (also recall (3) in Exercise 1.3.10). This shows (1.15).

(2) From (1) we get

$$A_1^2 = b_0A_0 + (b_0 - b_1 - c_1)A_1 + c_2A_2 \tag{1.19}$$

that is

$$A_2 = \frac{1}{c_2}A_1^2 - \frac{b_0 - b_1 - c_1}{c_2}A_1 - \frac{b_0}{c_2}I =: p_2(A_1),$$

and the general case follows by induction (note that as X is connected, one always has $c_2, c_3, \ldots, c_N > 0$). In particular, $\mathscr{A}$ is commutative. Moreover $\{A_0 = I, A_1, \ldots, A_N\}$ is a vector space basis for $\mathscr{A}$. Indeed, for any polynomial p one has that $p(A_1)$ is a linear combination of $A_0 = I, A_1, \ldots, A_N$ (this is a converse to (1): as in (1.19), it follows from a repeated application of (1.15)). Moreover, if $\alpha_0, \alpha_1, \ldots, \alpha_N \in \mathbb{C}$ and $x, y \in X$, one has

$$\left(\sum_{j=0}^{N} \alpha_j A_j \delta_y\right)(x) = \alpha_{d(x,y)}$$

https://doi.org/10.1017/9781009465939.002 Published online by Cambridge University Press

thus showing that $A_0, A_1, \dots, A_N$ are also independent. We deduce that $\dim(\mathscr{A}) = N+1$.

(3) Since $A_j = p_j(A_1)$ we have that V_i is also an eigenspace of the self-adjoint operator A_j with corresponding eigenvalue $p_j(\lambda_i)$ (below we shall prove that $n = N$). The fact that the eigenvalue λ_0 corresponding to the eigenspace V_0 equals the degree of X is nothing but a reformulation of the fact that, a graph X is connected (if and) only if 1 is an eigenvalue of multiplicity 1 of the Markov operator $M = \frac{1}{b_0}A_1$ (see Proposition 1.3.4).

(4) Denote by E_i the orthogonal projection onto V_i. From the preceding facts we deduce that $A_j = \sum_{i=0}^{n} p_j(\lambda_i)E_i$ for all $j = 0, 1, \dots, N$. As the spaces V_i's are orthogonal, the corresponding projections E_i's are independent. Moreover, they belong to $\mathscr{A}$ as they are expressed as polynomials in A_1:

$$E_i = \frac{\prod_{j\neq i}(A_1 - \lambda_j I)}{\prod_{j\neq i}(\lambda_i - \lambda_j)}. \tag{1.20}$$

As a consequence, the operators $E_0, E_1, \dots, E_n$ constitute another vector space basis for $\mathscr{A}$, and therefore $n = N$. $\square$

Let $\mathscr{G} = (X, E)$ be a distance-regular graph and set $d_i := \dim V_i$ (cf. (1.17)). From the above theorem it follows that there exist *real* coefficients $\phi_i(j)$, $i, j = 0, 1, \dots, N$ such that

$$E_i = \frac{d_i}{|X|}\sum_{j=0}^{N} \phi_i(j)A_j \tag{1.21}$$

for $i = 0, 1, \dots, N$.

Definition 1.3.12 (Spherical function on a distance-regular graph) The function $\phi_i \in L(\{0, 1, \dots, N\}$ is called the *spherical function* of X associated with V_i.

The factor $\frac{d_i}{|X|}$ in (1.21) is just a normalization constant.

The matrices

$$P = \left(p_j(\lambda_i)\right)_{j,i=0,1,\dots,N}$$

and

$$Q = \left(\frac{d_i}{|X|}\phi_i(j)\right)_{i,j=0,1,\dots,N}$$

are called the *first* and the *second eigenvalue matrix* of X, respectively.

Lemma 1.3.13 (1) *$P^{-1} = Q$ (that is $\frac{d_i}{|X|}\sum_{j=0}^{N}\phi_i(j)p_j(\lambda_h) = \delta_{i,h}$);*

(2) *$\phi_i(j) = \frac{1}{k_j}p_j(\lambda_i)$, where k_j is as in Exercise 1.3.10.(4), for all $i, j = 0, 1, \dots, N$;*

(3) *$\phi_0(j) = 1$ for all $j = 0, 1, \dots, N$;*

https://doi.org/10.1017/9781009465939.002 Published online by Cambridge University Press

(4) $\phi_i(0) = 1$ *for all* $i = 0, 1, \ldots, N$;
(5) $\lambda_i = b_0\phi_i(1)$.

Proof We leave the proof as an exercise (see [15, proof of Lemma 5.1.8]). □

Theorem 1.3.14 (1) *The spherical functions satisfy the following orthogonality relations:*

$$\sum_{j=0}^{N} k_j \phi_i(j)\phi_h(j) = \frac{|X|}{d_i}\delta_{i,h} \tag{1.22}$$

for all $i, h = 0, 1, \ldots, N$.

(2) *We have the following finite difference equations:*

$$c_j\phi_i(j-1) + (b_0 - b_j - c_j)\phi_i(j) + b_j\phi_i(j+1) = \lambda_i\phi_i(j) \tag{1.23}$$

for all $i, j = 0, 1, \ldots, N$ *(we use the convention that* $\phi_i(-1) = \phi_i(N+1) = 0$*).*

Proof (1) This is easily established by explicitly writing the coefficients in $QP = I$ and then using Lemma 1.3.13 in order to express $p_j(\lambda_i) = k_j\phi_i(j)$.

(2) From (1.18) and Lemma 1.3.13 we deduce

$$A_j = \sum_{i=0}^{N} k_j\phi_i(j)E_i. \tag{1.24}$$

From Proposition 1.3.11 and (1.24) we deduce

$$\begin{aligned} A_1A_j &= b_{j-1}A_{j-1} + (b_0 - b_j - c_j)A_j + c_{j+1}A_{j+1} = \\ &= \sum_{i=0}^{N} \big[b_{j-1}k_{j-1}\phi_i(j-1) + (b_0 - b_j - c_j)k_j\phi_i(j) + \\ &\qquad + c_{j+1}k_{j+1}\phi_i(j+1)\big]\, E_i. \end{aligned} \tag{1.25}$$

On the other hand, as $A_1E_i = E_iA_1 = \lambda_iE_i$ (recall that $A_1 = \sum_{i=0}^{N}\lambda_iE_i$), multiplying both sides of (1.24) by A_1 we obtain

$$A_1A_j = \sum_{i=0}^{N} k_j\phi_i(j)\lambda_iE_i. \tag{1.26}$$

Equating the two expressions of A_1A_j in (1.25) and (1.26) we obtain

$$b_{j-1}\frac{k_{j-1}}{k_j}\phi_i(j-1) + (b_0 - b_j - c_j)\phi_i(j) + c_{j+1}\frac{k_{j+1}}{k_j}\phi_i(j+1) = \lambda_i\phi_i(j).$$

Then (1.23) follows from Exercise 1.3.10.(4). □

In the monograph [53] one may find several examples of orthogonal polynomials satisfying systems of equations such as (1.23).

Example 1.3.15 (The discrete circle) As a first example of distance-regular graph, we examine the discrete circle $\mathscr{C}_n$ on $n \geq 3$ vertices. The vertex set $X := \{0,1,\dots,n-1\}$ and the edges are $e = \{x, x+1\}$ with $x \in X$ with summation modulo n. Clearly its diameter is given by $\mathrm{diam}(\mathscr{C}_n) = [n/2]$, the integer part of $n/2$. We leave it as an exercise to check that $\mathscr{C}_n$ is distance-regular with $N = [n/2]$ and parameters $b_0 = 2, b_1 = b_2 = \dots = b_{N-1} = 1$, $c_1 = c_2 = \dots = c_{N-1} = 1$ and, finally, $c_N = 1$ if n is odd and $c_N = 2$ if n is even.

In the present setting, the difference equations (1.23) become

$$\begin{cases} \phi_i(j-1) + \phi_i(j+1) = 2\phi_i(1)\phi_i(j) & \text{for } 1 \leq j \leq N-1 \\ \phi_i(N-1) + \phi_i(N) = 2\phi_i(1)\phi_i(N) & \text{if } n \text{ is odd} \\ 2\phi_i(N-1) = 2\phi_i(1)\phi_i(N) & \text{if } n \text{ is even} \end{cases}$$

for all $i = 0, 1, \dots, N$. Recalling the prosthaphæresis formula

$$\cos\alpha + \cos\beta = 2\cos((\alpha+\beta)/2)\cos((\alpha-\beta)/2)$$

we deduce that $\phi_i(j) = \cos(2\pi ij/n)$ for all $0 \leq i, j \leq N$.

Keeping in mind the decomposition (1.13) (where now "m" is replaced by "N"), we compute the dimension d_i of the subspaces V_i, for $i = 0, 1, \dots, N$. Suppose first that n is even, so that $N = n/2$. We have $k_0 = 1$ and, from the orthogonality relations (1.22), the parameters yield (cf. Exercise 1.3.10.(4))

$$k_i = b_0 b_1 \cdots b_{i-1} / c_2 c_3 \cdots c_i = 2$$

for all $1 \leq i \leq N-1$, and

$$k_N = b_0 b_1 \cdots b_{N-1} / c_2 c_3 \cdots c_N = 1.$$

We have $\dim(V_0) = 1$ (this is the dimension of the constant valued functions). Moreover, for $1 \leq i \leq N-1$ we have

$$\begin{aligned} \sum_{j=0}^{n/2} k_j \phi_i^2(j) &= \phi_i^2(0) + 2\sum_{j=1}^{n/2-1} \cos^2(2\pi ij/n) + \phi_i^2(n/2) \\ &= 2 + 2\sum_{j=1}^{n/2-1} \frac{1+\cos(4\pi ij/n)}{2} \\ &= 2 + (n/2-1) + \sum_{j=1}^{n/2-1} \cos(4\pi ij/n) \\ &= n/2 \equiv N, \end{aligned}$$

where, denoting by ω a primitive Nth root of unity, we used the equality

$$\sum_{j=1}^{n/2-1} \cos(4\pi ij/n) = \sum_{j=1}^{N-1} \cos(2\pi ij/N) = \Re(\omega + \omega^2 + \cdots + \omega^{N-1}) = -1.$$

We deduce that $d_i = n/(\sum_{j=0}^{n/2} k_j \phi_i^2(j)) = n/(n/2) = 2$. Finally, as $\phi_{n/2}^2(j) = 1$ for all $j = 0, 1, \ldots, n/2$, we deduce that $d_N = 1$.

We leave it as an exercise to check that, for n odd, one has $d_0 = 1$ and $d_i = 2$ for all $i = 1, 2, \ldots, N = (n-1)/2$.

Example 1.3.16 (Complete graph) The *complete graph* $K_n = (X, E)$ on n vertices is defined by setting $X := \{1, 2, \ldots, n\}$ and

$$E := \{\{x, y\} : x, y \in X,\ x \neq y\}$$

(Figure 1.2). It is clear that $N := \operatorname{diam}(K_n) = 1$ and that K_n is a distance regular graph with parameters $b_0 = n-1$, $b_1 = b_N = 0$, $c_0 = 0$, and $c_1 = 1$.

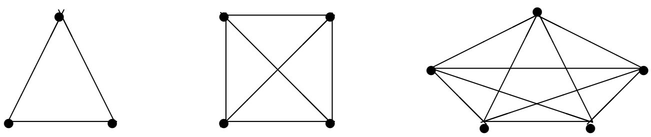

Figure 1.2 The complete graphs K_3, K_4, and K_5.

The decomposition (1.13) becomes $L(X) = \sum_{i=0}^{N} V_i = V_0 \oplus V_1$, where, as usual V_0 is the one-dimensional subspace of constant valued functions on X, and $V_1 = \{f \in L(X) : \sum_{x \in X} f(x) = 0\}$ is the (orthogonal) $(n-1)$-dimensional subspace of 0-mean-valued functions on X. The spherical functions $\phi_0, \phi_1 \in L(\{0,1\})$ are given by $\phi_0(j) = 1$ for $j = 0, 1$, and $\phi_1(0) = 1$ and $\phi_1(1) = -1/(n-1)$, as one easily deduces (exercise) from the orthogonality relations (1.22).

Example 1.3.17 (Hamming scheme and hypercube) Set $X_{n,m+1} := \{0, 1, 2, \ldots, m\}^n$. The map $d\colon X_{n,m+1} \times X_{n,m+1} \to \mathbb{N}$ defined by setting

$$d(x, y) := |\{k : x_k \neq y_k\}|$$

for all $x = (x_1, x_2, \ldots, x_n), y = (y_1, y_2, \ldots, y_n) \in X_{n,m+1}$, is easily seen to be a metric on $X_{n,m+1}$, called the *Hamming distance* on $X_{n,m+1}$.

We define a graph $\mathscr{G}_{n,m+1}^{\mathrm{H}} = (X_{n,m+1}, E_{n,m+1})$ by setting

$$E_{n,m+1} := \{\{x, y\} : x, y \in X_{n,m+1} \text{ such that } d(x, y) = 1\}.$$

https://doi.org/10.1017/9781009465939.002 Published online by Cambridge University Press

Then $\mathscr{G}^{\mathrm{H}}_{n,m+1}$ is a distance regular graph with diameter n and parameters

$$c_i = i, \qquad i = 1,2,\dots,n$$
$$b_i = (n-i)m, \qquad i = 0,1,\dots,n-1.$$

In particular, its degree is $b_0 = nm$. We leave it as an exercise to check for the details. See also page 134.

Note that for $n = 1$, the graph $\mathscr{G}^{\mathrm{H}}_{1,m+1}$ coincides with the complete graph K_{m+1} on $m+1$ vertices. Moreover, in this case, we always have $b_i + c_i = b_0$ (cf. Exercise 1.3.10).

For $m = 1$, the graph $\mathscr{G}^{\mathrm{H}}_{n,2}$ is called the *n-hypercube*, denoted Q_n (Figure 1.3).

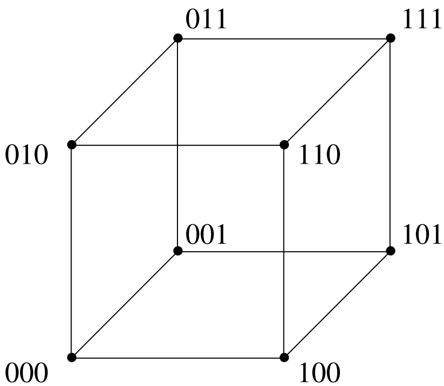

Figure 1.3 The 3-*hypercube* Q_3.

We refer to [15, Section 2.6 and Section 5.3] for the expressions of the spherical functions and the computation of the dimensions of the corresponding eigenspaces for Q_n and $\mathscr{G}^{\mathrm{H}}_{n,m+1}$, respectively. Note that the spherical functions constitute an important family of orthogonal polynomials, called the *Krawtchouk polynomials*.

Example 1.3.18 (Johnson scheme) Let n be a positive integer. For $0 \le m \le n$ denote by $\Omega_{m,n}$ the set of all m-subsets of $\{1,2,\dots,n\}$. The map $d\colon \Omega_{m,n} \times \Omega_{m,n} \to \mathbb{N}$ defined by setting

$$d(A,B) := m - |A \cap B|$$

for all $A, B \in \Omega_{m,n}$ is easily seen to be a metric on $\Omega_{m,n}$, called the *Johnson distance* on $\Omega_{m,n}$.

We define a graph $\mathscr{G}^{\mathrm{J}}_{m,n} = (\Omega_{m,n}, E_{m,n})$ by setting

$$E_{m,n} := \{\{A,B\} : A,B \in \Omega_{m,n} \text{ such that } d(A,B) = 1\}.$$

We leave it as an exercise to check that $\mathscr{G}^{\mathrm{J}}_{m,n}$ is a distance regular graph with diameter $\min\{m,n-m\}$ and parameters $c_i = i^2$ and $b_i = (n-m-i)(m-i)$ for $i = 0,1,\dots,\min\{m,n-m\}$.

We refer to [15, Section 6.1] for the expression of the spherical functions and the computation of the dimensions of the corresponding eigenspaces.

The book by Brouwer, Cohen, and Neumaier [8] is an encyclopedic treatment of distance-regular graphs.

1.3.2 Strongly regular graphs

This section is devoted to an interesting subclass of distance regular graphs (see also Section 2.5 for asymptotic aspects as well as Sections 3.2 and 3.4 for more combinatorial aspects of distance regular graphs).

Definition 1.3.19 A finite simple graph $\mathscr{G} = (X,E)$ without loops is called *strongly regular* with *parameters* (v,k,λ,μ) if

(1) it is regular of degree k and $|X| = v$;
(2) for all $\{x,y\} \in E$ there exist exactly λ vertices adjacent to both x and y;
(3) for all $x,y \in X$ with $x \neq y$ and $\{x,y\} \notin E$ there exist exactly μ vertices adjacent to both x and y.

It is customary to exclude graphs which satisfy the definition trivially, namely those graphs which are the disjoint union of one or more equal-sized complete graphs, and their complements (cf. Exercise 1.3.23 below). But we warn the reader that this convention is not adopted in Section 3.1.8, where these examples play an important role.

Note that, in the above definition, $0 \le \lambda \le k-1$ and $0 \le \mu \le k$. Moreover, if $\mu > 0$ then $\mathscr{G}$ is connected. In the following we shall always assume that $\mu > 0$.

Remark 1.3.20 Let $\mathscr{G} = (X,E)$ be a strongly regular graph with parameters (v,k,λ,μ) such that $\mu > 0$. By our assumptions on μ, given any two non-adjacent vertices there exists $z \in X$ such that $x \sim z$ and $z \sim y$, so that $d(x,y) = 2$. It follows that $N := \mathrm{diam}(\mathscr{G}) = 2$. Then, it is easy to check that $\mathscr{G}$ is a distance regular graph with parameters $(b_0,b_1,b_2) = (k,k-1-\lambda,0)$ and $(c_0,c_1,c_2) = (0,1,\mu)$.

Proposition 1.3.21 *Let $\mathscr{G} = (X,E)$ be a connected strongly regular graph with parameters (v,k,λ,μ) and denote by A its adjacency matrix. Let $L(X) =$*

https://doi.org/10.1017/9781009465939.002 Published online by Cambridge University Press

$V_0 \oplus V_1 \oplus V_2$ denote the decomposition (1.13)*, where, as usual V_0 is the one-dimensional subspace of constant-valued functions on X. The associated spherical function ϕ_0, ϕ_1, and ϕ_2 are given by*

- $\phi_0(j) = 1$ *for all* $j = 0, 1, 2$;
- $\phi_1(0) = 1$, $\phi_1(1) = \frac{\lambda-\mu+\sqrt{\Delta}}{2k}$, *and* $\phi_1(2) = -\frac{\mu(2+\lambda-\mu+\sqrt{\Delta})}{2k(k-1)}$;
- $\phi_2(0) = 1$, $\phi_2(1) = \frac{\lambda-\mu-\sqrt{\Delta}}{2k}$, *and* $\phi_2(2) = -\frac{\mu(2+\lambda-\mu-\sqrt{\Delta})}{2k(k-1)}$,

where $\Delta = (\lambda-\mu)^2 + 4(k-\mu)$. The dimensions $d_i = \mathrm{dim}(V_i)$, $i = 0, 1, 2$ are given by

- $d_0 = 1$;
- $d_1 = \frac{1}{2}\left[(v-1) - \frac{2k+(v-1)(\lambda-\mu)}{\sqrt{\Delta}}\right]$;
- $d_2 = \frac{1}{2}\left[(v-1) + \frac{2k+(v-1)(\lambda-\mu)}{\sqrt{\Delta}}\right]$.

Proof Formula (1.15) for $j = 1$ becomes (recall that $A = A_1$):

$$A^2 = kI + \lambda A + \mu(J - I - A)$$

which is equivalent to

$$A^2 + (\mu-\lambda)A + (\mu-k)I = \mu J,$$

where J is the $X \times X$ matrix consisting only of ones ($J_{x,y} = 1$ for all $x, y \in X$). Since the operator J, restricted to the subspace

$$L(X) \ominus V_0 := \{f \in L(x) : \sum_{x\in X} f(x) = 0\}$$

is the 0 operator, we deduce that the eigenvalues $t_1, t_2 \in \sigma(A) \setminus \{k\}$ satisfy the equation

$$t^2 + (\mu-\lambda)t + (\mu-k) = 0.$$

Therefore, up to a transposition of the indices, we have

$$t_1 := \frac{\lambda-\mu+\sqrt{\Delta}}{2} \quad \text{and} \quad t_2 := \frac{\lambda-\mu-\sqrt{\Delta}}{2}.$$

From Lemma 1.3.13(5), we obtain the above values $\phi_i(1)$ for $i = 1, 2$. Finally, the values of $\phi_i(2)$ for $i = 1, 2$ are easily deduced from the orthogonality relations (1.22).

For the dimensions of the eigenspaces, as usual we have $d_0 = \mathrm{dim}(V_0) = 1$. Moreover, from the identities $d_1 + d_2 = \mathrm{dim}(L(X)) - 1 = |X| - 1 = v - 1$ and $0 = \mathrm{tr}(A) = k + t_1 d_1 + t_2 d_2$ one deduces the corresponding expressions for d_1 and d_2. □

https://doi.org/10.1017/9781009465939.002 Published online by Cambridge University Press

Exercise 1.3.22 Let $m \geq 4$ and denote by X the set of all 2-element subsets of $\{1,2,\ldots,m\}$. The *triangular graph* $T(m)$ is the finite graph with vertex set X and such that two distinct vertices are adjacent if they are not disjoint.

Show that $T(m)$ is strongly regular with parameters $v = \binom{m}{2}$, $k = 2(m-2)$, $\lambda = m-2$, and $\mu = 4$.

Exercise 1.3.23 (Complement of a graph) Let $\mathscr{G} = (X,E)$ be a finite simple graph without loops. The *complement* of $\mathscr{G}$ is the graph $\overline{\mathscr{G}}$ with vertex set X and edge set $\overline{E} = \{\{x,y\} : x,y \in X, x \neq y, \{x,y\} \notin E\}$.

(1) Show that if $\mathscr{G}$ is strongly regular with parameters (v,k,λ,μ), then $\overline{\mathscr{G}}$ is strongly regular with parameters $(v, v-k-1, v-2k+\mu-2, v-2k+\lambda)$.
(2) From (1) deduce that the parameters of a strongly regular graph satisfy the inequality $v-2k+\mu-2 \geq 0$.
(3) Suppose that $\mathscr{G}$ is strongly regular. Show that $\mathscr{G}$ and $\overline{\mathscr{G}}$ are both connected if and only if $0 < \mu < k < v-1$. If this is the case, one says that $\mathscr{G}$ is *primitive*.
Hint: show that $\mu = 0$ implies $\lambda = k-1$ and write $\mu < k$ in the form $v-2k+\mu-2 < (v-k-1)-1$.

Example 1.3.24 (Petersen graph) The complement of the triangular graph $T(5)$ (see Exercise 1.3.22) is the celebrated *Petersen graph* (see Figure 1.4). It is a connected strongly regular graph with parameters $(10,3,0,1)$. The monograph [45] is entirely devoted to this graph which turned out to serve as a counterexample to several important conjectures.

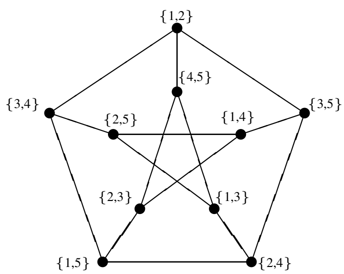

Figure 1.4 The Petersen graph

Example 1.3.25 (Clebsch graph) The *Clebsch graph* (see Figure 1.5) is defined as follows. The vertex set X consists of all subsets of even cardinality of the set $\{1,2,3,4,5\}$. Moreover, two vertices $A,B \in X$ are adjacent if $|A \triangle B| = 4$ (here $\triangle$ denotes the symmetric difference of two sets). We leave it as an exercise to show that it is a strongly regular graph with parameters $(16,5,0,2)$.

https://doi.org/10.1017/9781009465939.002 Published online by Cambridge University Press

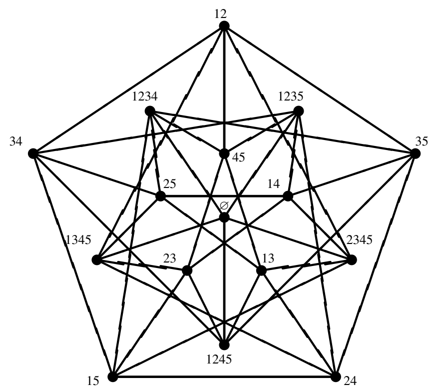

Figure 1.5 The Clebsch graph

For more on strongly regular graphs we refer to the monographs by van Lint and Wilson [49] and Godsil and Royle [42].

1.4 Association schemes

In this section we give the definition of an association scheme and discuss some examples. Association schemes constitute a central notion in Algebraic Combinatorics, which is "the approach to combinatorics – formulated in Ph. Delsarte's monumental and epochal thesis [25] in 1973 – enabling us to look at a wide range of combinatorial problems from a unified viewpoint" [3]. There are several beautiful books devoted to this subject: we mention, among others, those by Eiichi Bannai and Ito [3] and the new edition, written in collaboration with Etsuko Bannai and Rie Tanaka [4], Bailey [2], Godsil [41], van Lint and Wilson [49], Cameron [11], Cameron and van Lint [12], MacWilliams and Sloane [51], and by P.-H. Zieschang [73].

We finally present a generalization expressed in terms of hypergroups. We refer to the monograph [22] by Corsini and Leoreanu for a comprehensive treatment of the theory of hypergroups.

Definition 1.4.1 Let X be a finite set. An *association scheme* on X is a partition

$$X \times X = \mathscr{C}_0 \sqcup \mathscr{C}_1 \sqcup \ldots \sqcup \mathscr{C}_N,$$

where the sets $\mathscr{C}_i$ (called the *associate classes*) satisfy the following properties:

(1) $\mathscr{C}_0 = \{(x,x) : x \in X\}$ is the diagonal;

https://doi.org/10.1017/9781009465939.002 Published online by Cambridge University Press

(2) for each $i = 1, 2, \dots, N$, there exists i' with $1 \le i' \le N$ such that $\mathscr{C}_{i'} = \mathscr{C}_i^*$, where $\mathscr{C}_i^* := \{(y,x) \in X \times X : (x,y) \in \mathscr{C}_i\}$;

(3) there exist nonnegative integers (called the *parameters* of the scheme) $p_{i,j}^k$, $i, j, k = 0, 1, \dots, N$, such that

$$|\{z \in X : (x,z) \in \mathscr{C}_i, (z,y) \in \mathscr{C}_j\}| = p_{i,j}^k$$

for all $(x,y) \in \mathscr{C}_k$.

Moreover, the association scheme is called *commutative* (resp. *symmetric*) provided $p_{i,j}^k = p_{j,i}^k$ (resp. $\mathscr{C}_i = \mathscr{C}_i^*$; equivalently, $i' = i$) for all $1 \le i, j, k \le N$.

Note that symmetry implies commutativity.

Let X be a finite set and let $(\mathscr{C}_j)_{j=0}^N$ be an association scheme on X. For $j = 0, 1, \dots, N$, we define the matrix $A_j = (A_j(x,y))_{x,y \in X}$ by setting

$$A_j(x,y) := \begin{cases} 1 & \text{if } (x,y) \in \mathscr{C}_j \\ 0 & \text{otherwise.} \end{cases} \tag{1.27}$$

Note that $A_0 = I$. The subalgebra $\mathscr{A} \subseteq \mathrm{End}(L(X))$ generated by $A_0, A_1, \dots, A_N$ is called the *adjacency algebra* (or, when it is commutative, the *Bose–Mesner algebra*) associated with the association scheme $(\mathscr{C}_j)_{j=0}^N$ on X (see [3, 4, 2]). We remark that condition (3) in Definition 1.4.1 is equivalent to the following condition on $\mathscr{A}$:

$$A_i A_j = \sum_{k=0}^{N} p_{i,j}^k A_k \tag{1.28}$$

for all $0 \le i, j \le N$.

Example 1.4.2 (Groups as association schemes) Every finite group naturally gives rise to an association scheme over its underlying set. Indeed, given a finite group G, for $g \in G$ set

$$\mathscr{C}_g := \{(h,k) \in G \times G : h^{-1}k = g\}.$$

We then have, $\mathscr{C}_{1_G} = \{(g,g) : g \in G\}$ is the diagonal. Moreover, $\mathscr{C}_g^* = \mathscr{C}_{g^{-1}}$, in other words, $g' = g^{-1}$, for all $g \in G$. Finally, the parameters

$$p_{g,h}^k := \begin{cases} 1 & \text{if } k = gh \\ 0 & \text{otherwise,} \end{cases}$$

for all $g, h, k \in G$, trivially satisfy (3).

Note that G is commutative if and only if the corresponding association scheme is commutative. Also the association scheme is symmetric exactly if every nontrivial element in G has period 2 (that is, G is an elementary abelian 2-group).

We leave it as an easy exercise to check that the associated adjacency algebra $\mathscr{A}$ is isomorphic to the group algebra $L(G) = \{f\colon G \to \mathbb{C}\}$ of G (equipped with the convolution product (1.1)).

Example 1.4.3 (Association scheme associated with a group action) Let G be a finite group acting transitively on a set X. Consider the diagonal action of G on $X \times X$ and denote by $\mathscr{C}_0, \mathscr{C}_1, \ldots, \mathscr{C}_N$ (with $\mathscr{C}_0 = \{(x,x) : x \in X\}$) the corresponding orbits. Let us show that $\mathscr{C}_0, \mathscr{C}_1, \ldots, \mathscr{C}_N$ form an association scheme over X. The fact that $\mathscr{C}_0, \mathscr{C}_1, \ldots, \mathscr{C}_N$ form a partition of $X \times X$ and that $\mathscr{C}_0$ is the diagonal (cf. Definition 1.4.1(1)) immediately follows from the definitions. Let $1 \leq i \leq N$ and let $(x,y) \in \mathscr{C}_i$. Then denoting by $\mathscr{C}_{i'}$ the G-orbit of (y,x), we clearly have $\mathscr{C}_i^* = \mathscr{C}_{i'}$. This shows (2). Finally, let $1 \leq i,j,k \leq N$ and suppose that $(x,y), (x',y') \in \mathscr{C}_k$. Let $X_{x,y} := \{z \in X : (x,z) \in \mathscr{C}_i \text{ and } (z,y) \in \mathscr{C}_j\}$ and $X_{x',y'} := \{z' \in X : (x',z') \in \mathscr{C}_i \text{ and } (z',y') \in \mathscr{C}_j\}$. Let $g \in G$ such that $(gx, gy) = g(x,y) = (x',y')$. Then the map $\varphi\colon X_{x,y} \to X_{x',y'}$ defined by setting $\varphi(z) := gz$ for all $z \in X_{x,y}$ is well defined and bijective. Indeed, we have $(x,z) \in \mathscr{C}_i$ (resp. $(z,y) \in \mathscr{C}_j$) if and only if $(x', \varphi(z)) = g(x,z) \in \mathscr{C}_i$ (resp. $(\varphi(z), y') = g(z,y) \in \mathscr{C}_j$), and the inverse map is $\varphi^{-1}(z') := g^{-1}z'$ for all $z' \in X_{x',y'}$. This shows that the parameter $p_{i,j}^k$ is well defined, and (3) follows as well.

Let $x_0 \in X$ and denote by $K = \mathrm{Stab}_G(x_0)$ its stabilizer in G. We leave to the reader the following exercise:

(1) Show that the associated Bose–Mesner algebra $\mathscr{A}$ is isomorphic to the algebras $\mathrm{End}_G(L(X))$ and ${}^K L(G)^K$ (cf. Proposition 1.2.52 and its proof).
(2) Show that the association scheme in (1) is commutative if and only if (G,K) is a Gelfand pair.
(3) Show that the association scheme in (1) is symmetric if and only if (G,K) is a symmetric Gelfand pair (cf. Exercise 1.2.57).

Example 1.4.4 (Association scheme associated with conjugacy classes on a finite group) Let G be a finite group. Given $g \in G$, denote by $C(g) := \{h^{-1}gh : h \in G\}$ its conjugacy class. Let $C := \{C(g) : g \in G\}$ be the set of all conjugacy classes of G and denote by $c_0 := C(1_G) = \{1_G\}$ the conjugacy class of the identity element of G. Note that $C(g^{-1}) = \{h^{-1}g^{-1}h : h \in G\} = \{(h^{-1}gh)^{-1} : h \in G\} = C(g)^{-1}$ for all $g \in G$. For $c \in C$ we then set

$$\mathscr{C}_c := \{(x,y) \in G \times G : x^{-1}y \in c\}.$$

We have $\mathscr{C}_0 := \mathscr{C}_{c_0} = \{(g,g) : g \in G\}$ is the diagonal. Moreover, $\mathscr{C}_c^* = \mathscr{C}_{c^{-1}}$, in other words, $c' = c^{-1}$, for all $c \in C$. Let now $c_1, c_2, c_3 \in C$ and suppose that

https://doi.org/10.1017/9781009465939.002 Published online by Cambridge University Press

$(x_1,y_1),(x_2,y_2) \in \mathscr{C}_{c_1}$, that is, $x_i^{-1}y_i \in c_1$. Let also $z_1 \in G$. Then $(x_1,z_1) \in \mathscr{C}_{c_2}$ and $(z_1,y_1) \in \mathscr{C}_{c_3}$ if and only if $x_1^{-1}z_1 \in c_2$ and $z_1^{-1}y_1 \in c_3$; equivalently,

$$z_1 \in x_1c_2 \cap y_1(c_3)^{-1} = x_1(c_2 \cap x_1^{-1}y_1(c_3)^{-1}).$$

Analogously, for $z_2 \in G$ one has $(x_2,z_2) \in \mathscr{C}_{c_2}$ and $(z_2,y_2) \in \mathscr{C}_{c_3}$ if and only if $z_2 \in x_2(c_2 \cap (x_2)^{-1}y_2(c_3)^{-1})$. As $x_1^{-1}y_1,(x_2)^{-1}y_2 \in c_1$, there exists $t \in G$ such that $(x_2)^{-1}y_2 = t^{-1}(x_1^{-1}y_1)t$. We deduce that

$$\begin{aligned}
|x_1(c_2 \cap x_1^{-1}y_1(c_3)^{-1})| &= |c_2 \cap x_1^{-1}y_1(c_3)^{-1}| \\
&= |t^{-1}(c_2 \cap x_1^{-1}y_1(c_3)^{-1})t| \\
&= |c_2 \cap (x_2)^{-1}y_2(c_3)^{-1}| \\
&= |x_2(c_2 \cap (x_2)^{-1}y_2(c_3)^{-1})|.
\end{aligned}$$

This shows that the parameter $p_{c_2,c_3}^{c_1} = |c_2 \cap x^{-1}y(c_3)^{-1}|$ is well defined, that is, it does not depend on the choice of $(x,y) \in c_1$. This completes the proof that the $\mathscr{C}_c$s form an association scheme.

It is easy to see that the association scheme is commutative. Clearly, it is symmetric if and only if every $g \in G$ is conjugate to its inverse g^{-1}, a condition which is usually expressed by saying that the group G is *ambivalent*.

We leave it as an easy exercise to check that the associated Bose–Mesner algebra $\mathscr{A}$ is isomorphic to the subalgebra

$$L_c(G) := \{f \in L(G) : f(g) = f(h^{-1}gh) \text{ for all } g,h \in G\}$$

of *conjugacy-invariant functions* on G (equipped with the convolution product (1.1)).

Another interesting class of association schemes is provided by distance-regular graphs:

Proposition 1.4.5 (Distance-regular graphs are association schemes) *Let $\mathscr{G} = (X,E)$ be a distance-regular graph with diameter N, and set*

$$\mathscr{C}_i := \{(x,y) \in X \times X : d(x,y) = i\},$$

for $i = 0,1,\ldots,N$. Then $\mathscr{C}_0,\mathscr{C}_1,\ldots,\mathscr{C}_N$ form a symmetric association scheme over X.

Proof We clearly have (1) $\mathscr{C}_0 = \{(x,x) : x \in X\}$ is the diagonal and (2) $\mathscr{C}_i$ is *symmetric* for $i = 1,2,\ldots,N$. Consider the matrices $A_0,A_1,A_2,\ldots,A_N$ defined in (1.14). Recall that these constitute a vector space basis for the corresponding Bose–Mesner algebra $\mathscr{A} \subset \mathrm{End}(L(X))$ (cf. Proposition 1.3.11(2)). These are exactly the matrices defined in (1.14). In this setting, (1.28) (which is equivalent to condition (3) in Definition 1.4.1) follows from Proposition 1.3.11(2). □

As a consequence, the Hamming scheme (cf. Example 1.3.17) and the Johnson scheme (cf. Example 1.3.18) are symmetric (and therefore commutative) association schemes.

A peculiarity of a distance-regular graph is that, as remarked above (cf. Proposition 1.3.11(2)), its Bose–Mesner algebra is singly generated, namely by A_1. This is no longer true for general symmetric association schemes: see, for instance, [15, Chapter 7].

The following definition yields a generalization of the notion of an association scheme.

Definition 1.4.6 (Hypergroups) A finite *(algebraic) hypergroup* is a pair $(X,*)$, where X is a nonempty finite set equipped with a multi-valued map, called *hyperoperation* and denoted $*$, from $X \times X$ to $\mathscr{P}^*(X)$, the set of all nonempty subsets of X, satisfying the following properties:

(1) $(x*y)*z = x*(y*z)$ for all $x,y,z \in X$ (*associative property*);
(2) $x*X = X*x = X$ for all $x \in X$ (*reproduction property*),

where, for subsets $Y,Z \subset X$, one defines $Y*Z = \bigcup_{y\in Y, z\in Z} y*z \subset X$.

If, in addition one has

(3) $x*y = y*x$ for all $x,y \in X$ *(commutative property)*

one says that $(X,*)$ is commutative.

Also, an element $e \in X$ is called a *unit* provided that

(4) $x \in (e*x)\cap(x*e)$ for all $x \in X$.

Finally, given $x \in X$, an element $y \in X$ such that there is a unit e with

(5) $e \in (x*y)\cap(y*x)$

is called an *inverse* of x.

For another equivalent definition, under the name of *functional hypergroup*, we refer to [30, 31, 48] (see also [20, Appendix 3.3 and Example A.1]).

We remark that conditions (1), (4), and (5) imply condition (2). Suppose indeed that the hyperoperation $*$ is associative, that a unit $e \in X$ exists, and every element $x \in X$ has an inverse. Given $x,z \in X$, let $y \in X$ be an inverse of x. Then $x*X \supset x*(y*z) = (x*y)*z \supset (e*z) \ni z$, and, similarly, $X*x \ni z$. As z was arbitrary, this proves (2).

Example 1.4.7 (Association schemes are hypergroups) Let $\overline{X}$ be a finite set and let $\mathscr{C}_0, \mathscr{C}_1, \ldots, \mathscr{C}_N$ be an association scheme on $\overline{X}$. Set $X := \{\mathscr{C}_0, \mathscr{C}_1, \ldots, \mathscr{C}_N\}$. For $0 \le i, j \le N$ we set

$$\mathscr{C}_i * \mathscr{C}_j := \{\mathscr{C}_k : p_{i,j}^k \neq 0\}.$$

Let us show that $*$ is a hyperoperation turning $(X, *)$ into a hypergroup. Let A_j, $j = 0, 1, \ldots, N$ denote the matrices as in (1.27). Keeping in mind (1.28), the associative property of $*$ is easily deduced from the associative property of the product of matrices. Moreover, the element $e := \mathscr{C}_0$ is, clearly, a unit. Finally, it is straightforward that, for every $0 \le j \le N$, the class $\mathscr{C}_{j'} = \mathscr{C}_j^*$ is an inverse of $\mathscr{C}_j$. It follows from the above remark that $(X, *)$ is a hypergroup.

Example 1.4.8 (Dual of a finite group as hypergroup) Let G be a finite group. Then $X = \widehat{G}$, the dual of the group G, is an algebraic hypergroup after setting $x * y = \{z \in X : z \preceq x \otimes y\}$ for all $x, y \in X$. Moreover, the trivial representation $\iota_G \in X$ serves as a unit for the hypergroup and, given any $x \in X$, the conjugate representation $x' \in X$ (cf. Definition 1.2.10) serves as an inverse (cf. Exercise 1.2.47).

Finally in this section, we note that symmetric association schemes reappear in the definition of partially balanced designs in Section 3.1.8.

1.5 Applications of Gelfand pairs to probability

In this section, we illustrate the methods developed by Persi Diaconis and his collaborators which use representation theory of finite groups to determine the asymptotic behaviour of several mixing processes (typically finite Markov chains, e.g., random walks, invariant under the action of a finite group of symmetries). We illustrate this focusing on the Ehrenfest diffusion model which presents the so-called *cut-off phenomenon*. The standard reference is Diaconis' book [26]. We also based our exposition on our own monograph [15].

1.5.1 Markov chains

Definition 1.5.1 A *finite Markov chain* is a triple (X, P, ν_0), where X is a finite set, called the *state space*, $P = (p(x,y))_{x,y \in X}$, called the *transition matrix*, is a *stochastic matrix*, i.e.,

$$\begin{cases} p(x,y) \ge 0 & \text{for all } x, y \in X \\ \sum_{y \in X} p(x,y) = 1 & \text{for all } x \in X, \end{cases}$$

https://doi.org/10.1017/9781009465939.002 Published online by Cambridge University Press

and $\nu_0 \colon X \to [0,1]$, called the *initial distribution*, is a *probability distribution* on X, i.e.,

$$\begin{cases} \nu_0(x) \geq 0 & \text{for all } x \in X \\ \sum_{x \in X} \nu_0(x) = 1. \end{cases}$$

In the standard definition, a (discrete-time) Markov chain is a sequence of random variables $X_1, X_2, X_3, \ldots$ with the so-called *Markov property*, namely that the probability of moving to the next state depends only on the present state and not on the previous states, but, for our purposes, Definition 1.5.1 suffices. We can interpret a finite Markov chain (X, P, ν_0) as a *random walk* on X: at time $t = 0$ the random walker is in state $x = x(0)$ with probability $\nu_0(x)$. If at time t he or she is in state $x = x(t) \in X$, then at time $t+1$ he or she moves to state $y \in X$ with probability $p(x,y)$. Then, for $m \in \mathbb{N}$, the mth power matrix $P^m = \left(p^{(m)}(x,y)\right)$ is still stochastic and $p^{(m)}(x,y)$ is the probability of reaching state y at time $t+m$ given that at time t the random walker is in state x.

Definition 1.5.2 (mth iterate and uniform distributions) Let (X, P, ν_0) be a finite Markov chain. For $m \in \mathbb{N}$, the probability distribution $\nu^{(m)} := \nu_0 P^m$, that is,

$$\nu^{(m)}(x) := \sum_{y \in X} \nu_0(y) p^{(m)}(y,x)$$

for all $x \in X$, is called the mth *iterate distribution*.

The probability distribution $u \colon X \to [0,1]$ defined by setting $u(x) := \frac{1}{|X|}$ for all $x \in X$ is called the *uniform distribution* on X.

Remark 1.5.3 Note that the 0th iterate distribution satisfies $\nu^{(0)} \equiv \nu_0$. Moreover, $\mu * u = u$ for all probability distributions μ on X, where $*$ denotes the convolution product (cf. Example 1.2.13).

Definition 1.5.4 A stochastic matrix $P = (p(x,y))_{x,y \in X}$ is called *ergodic* (or *primitive*) if there exists m_0 such that $p^{(m_0)}(x,y) > 0$ for all $x, y \in X$.

Note that if a stochastic matrix P is ergodic and $p^{(m_0)}(x,y) > 0$ for all $x, y \in X$, then for all $m \geq m_0$ one has $p^{(m)}(x,y) > 0$ for all $x, y \in X$.

Given a finite Markov chain (X, P, ν_0), a probability distribution π is called a *stationary distribution* for P provided that $\pi P = \pi$, that is, $\sum_{y \in X} \pi(y) p(y,x) = \pi(x)$ for all $x \in X$.

Theorem 1.5.5 (Ergodic theorem) *Let (X, P, ν_0) be an ergodic Markov chain. Then there exists a unique, strictly positive, stationary distribution π for P and it is given as the limit of the mth iterate distributions, in formulæ,*

$$\lim_{m \to \infty} \nu^{(m)} = \pi.$$

https://doi.org/10.1017/9781009465939.002 Published online by Cambridge University Press

Proof We shall not prove this theorem in its full generality. The interested reader may find a complete proof in [15, Theorem 1.4.1]. However, we shall present a proof for two particular, yet significant, cases where equivalent conditions for ergodicity of the Markov chain are exploited (cf. Theorem 1.5.7 and Theorem 1.5.16). □

Definition 1.5.6 (Simple random walk on a finite regular graph) Let $\mathscr{G} = (X,E)$ be a k-regular finite graph. Given an initial distribution ν_0 on X, the associated *simple random walk* (*SRW*, for short) on $\mathscr{G}$ is the Markov chain (X,P,ν_0) where

$$p(x,y) := \begin{cases} 1/k & \text{if } x \sim y \\ 0 & \text{otherwise} \end{cases}$$

for all $x,y \in X$.

We remark that the simple random walk can be defined on any graph, not necessarily regular; the more general case has applications such as Jerrum's Markov chain for choosing a random orbit in a finite group action, or a random conjugacy class in a finite group [47].

Theorem 1.5.7 (Ergodic theorem for SRW on a regular graph) *Let $\mathscr{G} = (X,E)$ be a k-regular finite graph. Suppose that $\mathscr{G}$ is connected and not bipartite. Let (X,P,ν_0) denote the Markov chain associated with the simple random walk on $\mathscr{G}$ and initial distribution ν_0 on X. Then the mth iterate distributions converge to the uniform distribution u on X:*

$$\lim_{m\to\infty} \nu^{(m)} = u.$$

Proof Let $\lambda_0 \geq \lambda_1 \geq \lambda_2 \geq \cdots \geq \lambda_N$, where $N = |X|-1$, denote the eigenvalues of $P = (p(x,y))_{x,y\in X}$. Recall that $\lambda_0 = 1 > \lambda_1$ by Proposition 1.3.4, since $\mathscr{G}$ is connected, and $\lambda_N > -1$ by Proposition 1.3.8, since $\mathscr{G}$ is not bipartite. Since P is symmetric, we can find an orthogonal matrix O and a diagonal matrix D (whose diagonal entries are the eigenvalues) such that $P = ODO^t$. As a consequence, $P^n = OD^nO^t$, where the diagonal matrix D^n has, as diagonal entries, the nth powers of the eigenvalues $\lambda_0, \lambda_1, \ldots, \lambda_N$. Also recall that the columns of the orthogonal matrix O are exactly the normalized eigenvectors $v_0, v_1, \ldots, v_N \in \mathbb{R}^{N+1}$ corresponding to the eigenvalues $\lambda_0, \lambda_1, \ldots, \lambda_N$. In particular, $v_0 = (1/\sqrt{|X|}, 1/\sqrt{|X|}, \ldots, 1/\sqrt{|X|})$. As $\lambda_i^m \to 0$ as $m \to \infty$ for all $i = 1,2,\ldots,N$, then denoting by Q the diagonal matrix with 1 at position $(0,0)$

and vanishing elsewhere, we deduce that

$$\begin{aligned}\lim_{m\to\infty} P^m &= \lim_{m\to\infty} OD^m O^t\\ &= O(\lim_{m\to\infty} D^m)O^t\\ &= OQO^t\\ &= \Pi\end{aligned}$$

where $\Pi_{x,y} = 1/|X|$ for all $x, y \in X$. □

Note that, since $u(x) > 0$ for all $x \in X$, from the sign-permanence theorem we deduce that the Markov chain P in the theorem above is ergodic.

Definition 1.5.8 Let X be a finite set and let G be a finite group acting on X. A stochastic matrix $P = (p(x,y))_{x,y\in X}$ is *G-invariant* provided that $p(gx, gy) = p(x,y)$ for all $x, y \in X$ and $g \in G$.

Exercise 1.5.9 Let (X,d) be a metric space. Let G be a finite group acting isometrically on (X,d). Show that a stochastic matrix $P = (p(x,y))_{x,y\in X}$ is G-invariant if and only if $p(x,y)$ depends only on $d(x,y)$ for all $x, y \in X$.

Proposition 1.5.10 *Let X be a finite set and let G be a finite group acting on X. Let $P = (p(x,y))_{x,y\in X}$ be a G-invariant stochastic matrix. Let $x_0 \in X$ and set $K := \mathrm{Stab}_G(x_0)$. Then the map $\nu\colon X \to [0,1]$ defined by $\nu(x) = p(x_0,x)$ for all $x \in X$ is a K-invariant probability distribution on X and (cf. the notation in Definition 1.2.76)*

$$p^{(m)}(x_0,x) = \nu^{*m}(x)$$

for all $x \in X$ and $m \in \mathbb{N}$.

Proof We limit ourselves to show the equality for the case $m = 2$. Let $x \in X$ and let $g \in G$ such that $x = gx_0$. Then, using G-invariance of P in lines 4 and 7,

https://doi.org/10.1017/9781009465939.002 Published online by Cambridge University Press

and $y = hx_0$ in line 5,

$$\begin{aligned}
\nu^{*2}(x) &= [\nu * \nu](x) \\
&= \frac{1}{|K|} \sum_{h \in G} \widetilde{\nu}(gh) \widetilde{\nu}(h^{-1}) \\
&= \frac{1}{|K|} \sum_{h \in G} p(x_0, ghx_0) p(x_0, h^{-1}x_0) \\
&= \frac{1}{|K|} \sum_{h \in G} p(g^{-1}x_0, hx_0) p(hx_0, x_0) \\
&= \sum_{y \in X} p(g^{-1}x_0, y) p(y, x_0) \\
&= p^{(2)}(g^{-1}x_0, x_0) \\
&= p^{(2)}(x_0, gx_0) \\
&= p^{(2)}(x_0, x).
\end{aligned}$$

We leave it to the reader to prove the general case. □

The following is immediate.

Corollary 1.5.11 *Let (X, P, ν_0) be a finite Markov chain and let G be a finite group acting on X. Suppose that P is G-invariant. Fix $x_0 \in X$ and set $K = \mathrm{Stab}_G(x_0)$. Then the map $\nu \colon X \to [0,1]$ defined by $\nu(x) = p(x_0, x)$ for all $x \in X$ is a K-invariant probability distribution on X and*

$$\nu^{(m)} = \nu_0 * \nu^{*m} \tag{1.29}$$

for all $m \geq 1$ (cf. Definitions 1.5.2 and 1.2.76). □

Proposition 1.5.12 *Let (X, P, ν_0) be a Markov chain. Let G be a finite group acting on X. Let $x_0 \in X$ and set $K = \mathrm{Stab}_G(x_0)$. Suppose that (G, K) is a Gelfand pair and denote by $\phi_0 = 1, \phi_1, \ldots, \phi_N$ and by $d_0 = 1, d_1, \ldots, d_N$ the spherical functions and the dimensions of the corresponding spherical representations. Then*

$$\nu^{*m} = \frac{1}{|X|} \sum_{i=0}^{N} d_i \left[(\mathscr{F}\nu)(i) \right]^m \check{\phi}_i \tag{1.30}$$

and

$$\| \nu^{*m} - u \|_{L(X)}^2 = \frac{1}{|X|} \sum_{i=1}^{N} d_i \left[(\mathscr{F}\nu)(i) \right]^{2m}, \tag{1.31}$$

where u denotes the uniform distribution on X.

Proof Formula (1.30) follows immediately from the inversion formula (1.10) and the property (1.11).

We now observe that $u = \frac{\check{\phi}_0}{|X|}$ so that, by (1.30), we have

$$\nu^{*m} - u = \frac{1}{|X|} \sum_{i=1}^{N} d_i \, [(\mathscr{F}\nu)(i)]^m \, \check{\phi}_i.$$

Formula (1.31) then follows from the orthogonality relations for the spherical functions. □

Definition 1.5.13 Let X be a finite set. The *total variation distance* of two probability measures μ and ν on X is

$$\|\mu - \nu\|_{TV} := \max_{A \subseteq X} \left| \sum_{x \in A} (\mu(x) - \nu(x)) \right| = \max_{A \subseteq X} |\mu(A) - \nu(A)|.$$

Exercise 1.5.14 Given $f \in L(X)$ we denote by $\|f\|_{L^1(X)} := \sum_{x \in X} |f(x)|$ its L^1-norm. Show that $\|\mu - \nu\|_{TV} = \frac{1}{2}\|\mu - \nu\|_{L^1(X)}$.

The following is the celebrated upper bound lemma of Diaconis and Shahshahani.

Corollary 1.5.15 (Upper bound lemma) *With the same notation as in Proposition 1.5.12,*

$$\|\nu^{*m} - u\|_{TV}^2 \le \frac{1}{4} \sum_{i=1}^{N} d_i \, |\mathscr{F}\nu(i)|^{2m},$$

where u is the uniform distribution on X.

Proof Using the Cauchy–Schwarz inequality in the second line and (1.31) in the third,

$$\begin{aligned} \|\nu^{*k} - u\|_{TV}^2 &= \frac{1}{4} \|\nu^{*m} - u\|_{L^1(X)}^2 \\ &\le \frac{1}{4} \|\nu^{*m} - u\|^2 \cdot |X| \\ &= \frac{1}{4} \sum_{i=1}^{N} d_i \, |\mathscr{F}\nu(i)|^{2m}. \end{aligned}$$

□

We define the *support* of $f \in L(X)$ as the subset of X given by $\mathrm{supp}(f) := \{x \in X : f(x) \neq 0\} \subseteq X$.

Theorem 1.5.16 *Let (X, P, ν_0) be a Markov chain. Let G be a finite group acting on X and suppose that P is G-invariant. Let $x_0 \in X$ and set $K = \mathrm{Stab}_G(x_0)$. Suppose that (G, K) is a Gelfand pair and denote by $\phi_0 = 1, \phi_1, \ldots, \phi_N \in {}^K L(X)$*

https://doi.org/10.1017/9781009465939.002 Published online by Cambridge University Press

the associated spherical functions. Suppose that there exists $m_0 \geq 1$ *such that* $\mathrm{supp}(\nu^{*m_0}) = X$*. Then the mth iterates* $\nu^{(m)}$ *converge to the uniform distribution u on* X*.*

Proof By virtue of the upper bound lemma (cf. Corollary 1.5.15) and (1.29) combined with Remark 1.5.3, it suffices to show that $|\mathscr{F}\nu(i)| < 1$ for all $i = 1,2,\dots,N$. Since $\mathscr{F}\nu^{*m} = (\mathscr{F}\nu)^m$ for all $m \in \mathbb{N}$ (cf. Exercise 1.2.77), the above condition is clearly equivalent to $|\mathscr{F}\nu^{*m_0}(i)| < 1$ for all $i = 1,2,\dots,N$. Since $\mathrm{supp}(\nu^{*m_0}) = X$, this follows from the expression of $\mathscr{F}\nu^{*m_0}$ after observing that the spherical functions ϕ_i with $i \geq 1$ satisfy (i) $|\phi_i(x)| \leq 1$, (ii) $\phi_i(x_0) = 1$, and (iii) there exists $y \in X$ such that $\Re\phi_i(y) < 0$ (the latter follows from (ii) and $\sum_{x\in X} \phi_i(x) = 0$). $\square$

1.5.2 The Ehrenfest diffusion model

The Ehrenfest model of diffusion was proposed by Paul and Tatiana Ehrenfest in 1907 [35] to explain the second law of thermodynamics. We are given two urns numbered 0 and 1 and n balls numbered $1,2,\dots,n$. A *configuration* is a placement of the balls into the urns: there are 2^n configurations (2 choices for each ball).

The *configuration space* is $X = \mathscr{P}(\{1,2,\dots,n\})$, the set of all subsets of $\{1,2,\dots,n\}$: a subset $A \subseteq \{1,2,\dots,n\}$ corresponds to the balls contained in urn 0 (the remaining balls, namely those in $\{1,2,\dots,n\} \setminus A$, are in urn 1).

The *initial configuration* is $A_0 = \{1,2,\dots,n\}$: at time $t = 0$ all balls are in urn 0, while urn 1 is empty (Figure 1.6).

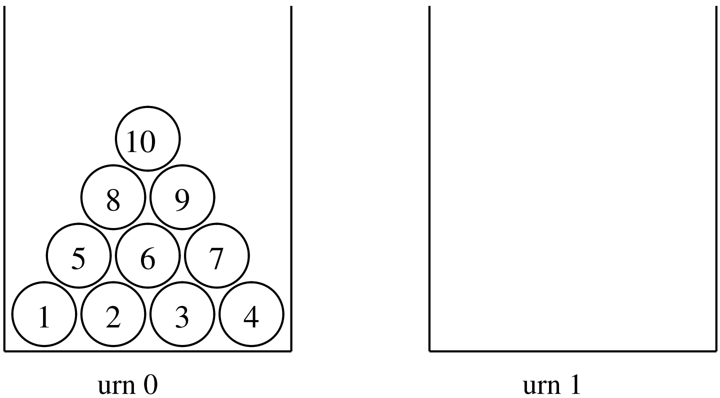

Figure 1.6 The *initial configuration* for the Ehrenfest diffusion model

https://doi.org/10.1017/9781009465939.002 Published online by Cambridge University Press

Then, at each time t, a ball is randomly chosen (each ball might be chosen with probability $1/n$) and it is moved to the other urn (Figures 1.7 and 1.8).

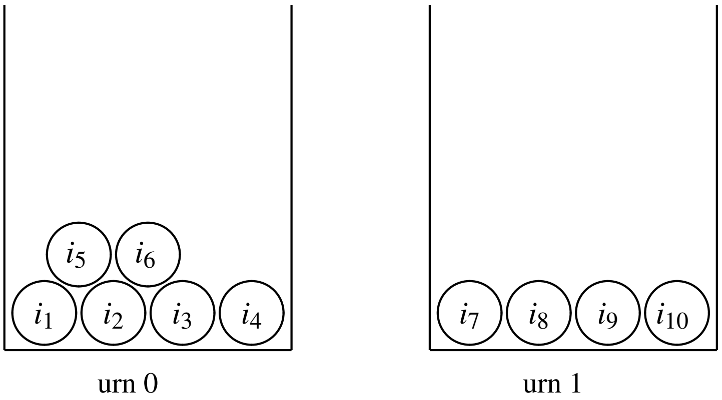

Figure 1.7 A configuration at time t in the Ehrenfest diffusion model

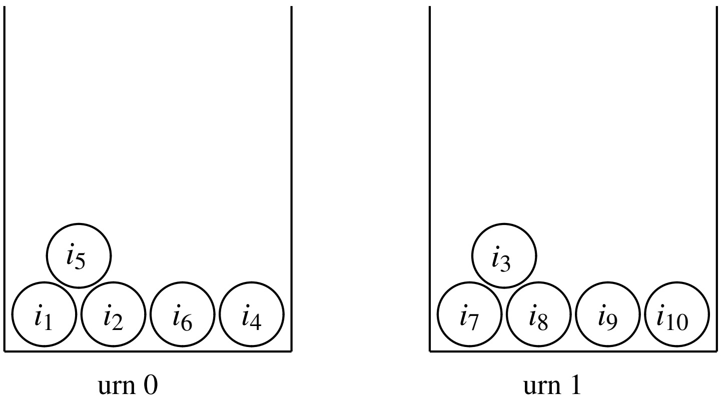

Figure 1.8 The configuration at time $t+1$ if the chosen ball is i_3

This process can be seen as a Markov chain on X with initial probability

https://doi.org/10.1017/9781009465939.002 Published online by Cambridge University Press

distribution $\nu_0 = \delta_{A_0}$, the Dirac delta at A_0, and transition matrix P' given by

$$p'(A,B) = \begin{cases} \frac{1}{n} & \text{if } |A \triangle B| = 1 \\ 0 & \text{otherwise} \end{cases}$$

for all $A, B \in X$, where $A \triangle B = (A \setminus B) \cup (B \setminus A)$ is the symmetric difference of A and B. Since the above stochastic matrix is not ergodic ($((p')^{(2n+1)}(A,A) = 0$ for all $A \in X$), we will consider a slight variation, namely the stochastic matrix P defined by

$$p(A,B) = \begin{cases} \frac{1}{n+1} & \text{if } |A \triangle B| = 1 \\ \frac{1}{n+1} & \text{if } A = B \\ 0 & \text{otherwise;} \end{cases}$$

in other words at each time t we allow the possibility (with probability $\frac{1}{n+1}$) to remain in the same state (i.e., to not change the configuration at time t).

Define the *Hamming distance* d_H on $\{0,1\}^n$ by setting

$$d_H((a_1,a_2,\ldots,a_n),(b_1,b_2,\ldots,b_n)) = |\{k \in \{1,2,\ldots,n\} : a_k \neq b_k\}|$$

for all $(a_1,a_2,\ldots,a_n),(b_1,b_2,\ldots,b_n) \in \{0,1\}^n$ (cf. Example 1.3.17). The metric space $Q_n = (\{0,1\}^n, d_H)$ is called the n-dimensional *hypercube*. We then regard Q_n as an undirected graph with loops, with vertex set $\{0,1\}^n$ and edges the pairs of vertices with Hamming distance equal to either 0 or 1. (This is the usual hypercube graph with a loop at each vertex.) We then identify X and Q_n via the bijection $\Phi \colon X \to Q_n$ given by

$$\Phi(A) = (a_1,a_2,\ldots,a_n), \quad \text{where } a_k = \begin{cases} 1 & \text{if } k \in A \\ 0 & \text{if } k \notin A. \end{cases}$$

Note that $|A \triangle B| = d_H(\Phi(A),\Phi(B))$ for all $A, B \in X$. This way, the Ehrenfest diffusion model (with n balls) can be seen as the *simple random walk* on the hypercube Q_n.

The wreath product $G = S_2 \wr S_n = (S_2 \times S_2 \times \cdots \times S_2) \rtimes S_n$ acts on Q_n by setting

$$(\sigma_1,\sigma_2,\ldots,\sigma_n;\theta)(a_1,a_2,\ldots,a_n) = (\sigma_1 a_{\theta^{-1}(1)}, \sigma_2 a_{\theta^{-1}(2)}, \ldots, \sigma_n a_{\theta^{-1}(n)})$$

for all $\sigma_i \in S_2$, $\theta \in S_n$, $a_i \in \{0,1\}$, and $i = 1,2,\ldots,n$.

Exercise 1.5.17 Show that the above action is isometric and two-point homogeneous.

Let $x_0 = (0,0,\ldots,0) \in Q_n$ and set $K = \mathrm{Stab}_G(x_0) \cong S_n$. From the above exercise we deduce that $(G,K) = (S_2 \wr S_n, S_n)$ is a symmetric Gelfand pair.

Set

$V_0 = \{f \in L(\{0,1\}) : f \text{ is constant}\}$ and $V_1 = \{f \in L(\{0,1\}) : f(0) + f(1) = 0\}$.

Then we have the orthogonal decomposition $L(\{0,1\}) = V_0 \oplus V_1$ into S_2-irreducible representations and, in turn,

$$L(Q_n) = L(\{0,1\}^n) \equiv (L(\{0,1\}))^{\otimes n} = (V_0 \oplus V_1)^{\otimes n}.$$

Setting $W_j = \mathrm{span}\{f_1 \otimes f_2 \otimes \cdots \otimes f_n : f_i \in V_0 \cup V_1, |\{i : f_i \in V_1\}| = j\}$, for $j = 0, 1, \ldots, n$, we have:

Theorem 1.5.18 *$L(Q_n) = \bigoplus_{j=0}^n W_j$ is the decomposition into $(S_2 \wr S_n)$-irreducible pairwise inequivalent sub-representations.*

The jth spherical function *$\phi_j \in W_j$ is*

$$\phi_j(g) = \frac{1}{\binom{n}{j}} \sum_{t=\max\{0, j-n+\ell\}}^{\min\{\ell, j\}} (-1)^t \binom{\ell}{t} \binom{n-\ell}{j-t},$$

where $\ell = d_h(gx_0, x_0)$, for all $g \in G$.

Proof See [15, Proposition 5.4.3]. □

We refer to [13, 18] for a far-reaching generalization of the decomposition of $L(Q_n)$ in the above theorem.

Remark 1.5.19 The functions ϕ_j are the so-called *Krawtchouk polynomials*.

The following theorem describes a very interesting feature for the asymptotics of the Ehrenfest diffusion process.

Theorem 1.5.20 (Diaconis–Shahshahani) *With the above notation we have the following.*

(1) *For $k = \frac{1}{4}(n+1)(\log n + c)$ with $c > 0$*

$$\|\nu^{*k} - u\|_{TV}^2 \leq \frac{1}{2}(e^{e^{-c}} - 1).$$

(2) *For $k = \frac{1}{4}(n+1)(\log n - c)$ with $c \in (0, \log n)$ and n large*

$$\|\nu^{*k} - u\|_{TV} \geq 1 - 20e^{-c}.$$

Proof See [15, Theorem 2.4.3]. Note that the Upper bound lemma (Corollary 1.5.15) plays a crucial role. □

The above theorem shows that $k^* = \frac{1}{4}(n+1)\log(n)$ steps are necessary and sufficient to reach the uniform distribution in the Ehrenfest model of diffusion. Moreover, the so-called *cut-off phenomenon* occurs (see Figure 1.9): the transition from order to chaos is concentrated in a small neighborhood of time $t = k^*$.

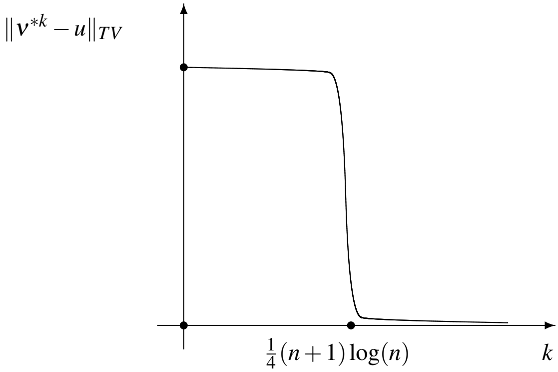

Figure 1.9 The cut-off phenomenon.

1.6 Induced representations and Mackey theory

This section is devoted to the basic theory of induced representations. We reformulate the classical Mackey theory, developed by Mackey in the setting of locally compact groups, in the finite group case. In particular, we present the *Little Group Method* due to Mackey and Wigner. Standard references for induced representations are the monographs by: Alperin and Bell [1], Fulton and Harris [39], Isaacs [46], Naimark and Stern [52], Serre [65], Simon [66], and Sternberg [68]. See also our monographs [16, 18, 19, 20] as well as the research-expository paper [17]. Finally, we generalize the notion of a finite Gelfand pair by introducing the reader to the theory of *multiplicity-free triples* developed in [20], where the role of the classical commutant $\mathrm{End}_G(L(G/K))$ is now played by a so-called *Hecke algebra*.

1.6.1 Induced representations

Definition 1.6.1 Let G be a finite group and let $K \leq G$ be a subgroup. The *induced representation* of a K-representation (σ, V) is the G-representation

$(\mathrm{Ind}_K^G \sigma, \mathrm{Ind}_K^G V)$ defined by setting

$$\mathrm{Ind}_K^G V = \{f \in V[G] : f(gk) = \sigma(k^{-1})f(g), \text{ for all } g \in G, k \in K\},$$

where $V[G]$ is the complex vector space of all functions $f\colon G \to V$, and

$$[\mathrm{Ind}_K^G \sigma(g_1)f](g_2) = f(g_1^{-1}g_2), \qquad \text{for all } g_1, g_2 \in G \text{ and } f \in \mathrm{Ind}_K^G V. \quad (1.32)$$

In the following, to simplify notation, we write $\lambda = \mathrm{Ind}_K^G \sigma$.

Exercise 1.6.2 With the above notation, prove the following.

- λ is a representation. (In particular, check that $\lambda(g)f \in \mathrm{Ind}_K^G V$ for all $g \in G$ and $f \in \mathrm{Ind}_K^G V$).
- Suppose that V is equipped with a scalar product $\langle \cdot, \cdot \rangle_V$ and that σ is unitary. Define a scalar product in $\mathrm{Ind}_K^G V$ by setting

$$\langle f_1, f_2 \rangle_{\mathrm{Ind}_K^G V} = \frac{1}{|K|} \sum_{g \in G} \langle f_1(g), f_2(g) \rangle_V$$

  for all $f_1, f_2 \in \mathrm{Ind}_K^G V$. Show that λ is unitary.

Remark 1.6.3 The following yields an alternative approach to the definition of an induced representation. For $v \in V$ define $f_v \in V[G]$ by setting

$$f_v(g) = \begin{cases} \sigma(g^{-1})v & \text{if } g \in K \\ 0 & \text{otherwise.} \end{cases} \quad (1.33)$$

It is straightforward to check that $f_v \in \mathrm{Ind}_K^G V$. Moreover, the set

$$\widetilde{V} = \{f_v : v \in V\} \subseteq \mathrm{Ind}_K^G V$$

is a K-invariant subspace of $\mathrm{Ind}_K^G V$ and $(\lambda|_K, \widetilde{V}) \sim (\sigma, V)$: indeed,

$$\lambda(k) f_v = f_{\sigma(k)v}$$

for all $k \in K$ and $v \in V$. Moreover, if $\mathscr{T} \subseteq G$ denotes a complete set of representatives for the left cosets of K in G, so that

$$G = \sqcup_{t \in \mathscr{T}} tK, \quad (1.34)$$

then we have

$$\mathrm{Ind}_K^G V = \bigoplus_{t \in \mathscr{T}} \lambda(t) \widetilde{V}. \quad (1.35)$$

It follows immediately from (1.35) and the equality $|\mathscr{T}| = [G : K]$, the *index* of K in G, that

$$\dim \mathrm{Ind}_K^G V = [G : K] \dim V. \quad (1.36)$$

https://doi.org/10.1017/9781009465939.002 Published online by Cambridge University Press

Exercise 1.6.4 (Induction in stages) Let $K \le H \le G$ be three groups and let (σ, V) be a K-representation. Then

$$\mathrm{Ind}_K^G \sigma \sim \mathrm{Ind}_H^G \mathrm{Ind}_K^H \sigma.$$

Hint: use the equivalence $(V[H])[G] \sim V[G \times H]$.

Example 1.6.5 Suppose that G acts transitively on a set X, let $x_0 \in X$, and set $K = \mathrm{Stab}_G(x_0)$. Recall (cf. Definition 1.2.50) that the permutation representation $(\lambda, L(X))$ is the G-representation defined by setting

$$[\lambda(g)f](x) = f(g^{-1}x)$$

for all $g \in G$, $x \in X$, and $f \in L(X)$. Then, denoting by $(\iota_K, \mathbb{C})$, the trivial representation of the group K, we have

$$\mathrm{Ind}_K^G \mathbb{C} = \{f \in L(G) : (\forall g \in G, k \in K)\, f(gk) = \iota_K(k) f(g) \equiv f(g)\} = L(G)^K.$$

So the map taking $f \in L(X)$ to $\widetilde{f} \in L(G)^K$ establishes an equivalence between $(\lambda, L(G/K))$ and $(\mathrm{Ind}_K^G \iota_K, \mathrm{Ind}_K^G \mathbb{C})$.

Example 1.6.6 Let $N \trianglelefteq G$ be a normal subgroup of G. Then, the corresponding homogeneous space $X = G/N$ has a natural structure of a group. Let $(\overline{\lambda_{G/N}}, L(G/N))$ be the G-representation defined by setting $\overline{\lambda_{G/N}}(g) = \lambda_{G/N}(gN)$ for all $g \in G$, where $\lambda_{G/N}$ denotes, as usual, the left regular representation of the group G/N. Then

$$(\lambda, L(X)) \equiv (\overline{\lambda_{G/N}}, L(G/N)).$$

Remark 1.6.7 More generally, if (σ, V) is a G/N-representation, its *inflation* $(\overline{\sigma}, V)$ is the G-representation defined by setting

$$\overline{\sigma}(g) = \sigma(gN) \tag{1.37}$$

for all $g \in G$.

Theorem 1.6.8 (Matrix coefficients) *Let $K \le G$ and let $\mathscr{T} \subseteq G$ as in* (1.34). *Given a K-representation (σ, V), take an orthonormal basis $\{e_1, e_2, \dots, e_d\}$ of V. Then*

$$\{f_{t,j} := \lambda(t) f_{e_j} : t \in \mathscr{T}, j = 1, 2, \dots, d\}$$

constitutes an orthonormal basis of $\mathrm{Ind}_K^G V$. *Moreover, the corresponding matrix coefficients are given by*

$$\left\langle \lambda(g) f_{t,j}, f_{s,i} \right\rangle_{\mathrm{Ind}_K^G V} = \begin{cases} \left\langle \sigma(s^{-1}gt) e_j, e_i \right\rangle_V & \text{if } s^{-1}gt \in K \\ 0 & \text{otherwise,} \end{cases}$$

for all $s, t \in \mathscr{T}$, $1 \le i, j \le d$, and $g \in G$.

Corollary 1.6.9 (Frobenius character formula) *With the notation of the above theorem, we have*

$$\chi^{\mathrm{Ind}_K^G \sigma}(g) = \sum_{\substack{t \in \mathscr{T}: \\ t^{-1}gt \in K}} \chi^{\sigma}(t^{-1}gt)$$

for all $g \in G$. □

Theorem 1.6.10 *Let (θ, W) be a G-representation and let (σ, V) be a K-representation, where $K \leq G$. Then*

$$W \otimes \mathrm{Ind}_K^G V \cong \mathrm{Ind}_K^G(\mathrm{Res}_K^G W \otimes V).$$

Proof Define $\phi : W \otimes \mathrm{Ind}_K^G V \to \mathrm{Ind}_K^G(\mathrm{Res}_K^G W \otimes V)$ by setting

$$\phi(w \otimes f)(g) = \theta(g^{-1})w \otimes f(g)$$

for all $g \in G, w \in W$ and $f \in \mathrm{Ind}_K^G V$. We leave it as an exercise to check that ϕ is bijective, and furthermore that it is an intertwiner between $\theta \otimes \mathrm{Ind}_K^G \sigma$ and $\mathrm{Ind}_K^G(\mathrm{Res}_K^G \theta \otimes \sigma)$. □

From the above theorem, with $(\sigma, V) = (\iota_K, \mathbb{C})$ and setting $X = G/K$, we immediately deduce the following important relation between induction and restriction:

Corollary 1.6.11

$$W \otimes L(X) \cong \mathrm{Ind}_K^G \mathrm{Res}_K^G W.$$ □

1.6.2 Mackey theory

Theorem 1.6.12 (Frobenius reciprocity) *Let (θ, W) be a G-representation and let (σ, K) be a K-representation, where $K \leq G$. Then, as vector spaces,*

$$\mathrm{Hom}_G(W, \mathrm{Ind}_K^G V) \cong \mathrm{Hom}_K(\mathrm{Res}_K^G W, V).$$

Proof For $T \in \mathrm{Hom}_G(W, \mathrm{Ind}_K^G V)$, define $\widehat{T} : W \to V$ by setting $\widehat{T}w = [Tw](1_G)$ for all $w \in W$. We leave it as an exercise to check that $\widehat{T} \in \mathrm{Hom}_K(\mathrm{Res}_K^G W, V)$.

Vice versa, for $S \in \mathrm{Hom}_K(\mathrm{Res}_K^G W, V)$, we define $\check{S}$: $W \to V[G]$ by setting $[\check{S}w](g) = S(\theta(g^{-1}w)$ for all $g \in G$ and $w \in W$. Again, it is easy to check that $\check{S} \in \mathrm{Hom}_G(W, \mathrm{Ind}_K^G V)$. Moreover, $(\hat{T})\check{} = T$ and $(\check{S})\hat{} = S$. These facts, and the obvious linearity of the maps $\hat{}$ and $\check{}$, end the proof. □

Remark 1.6.13 Let (ρ_1, V_1) and (ρ_2, V_2) be two G-representations and suppose that ρ_1 is irreducible. Then the multiplicity $m_{\rho_1}^{\rho_2}$ of ρ_1 in ρ_2 equals the dimension of $\mathrm{Hom}_G(V_1, V_2)$. See [19, Lemma 10.6.1.(i)].

From the remark and Frobenius reciprocity we immediately deduce:

Corollary 1.6.14 *Let* $(\theta, W) \in \widehat{G}$ *and let* $(\sigma, K) \in \widehat{K}$. *Then*

$$m_\theta^{\mathrm{Ind}_K^G \sigma} = m_\sigma^{\mathrm{Res}_K^G \theta}.$$

Let G be a group and let $H, K \leq G$ be two subgroups of G. Denote by $\mathscr{S}$ a complete set of representatives of the double cosets $H \backslash G / K$ so that $G = \sqcup_{s \in \mathscr{S}} HsK$. We suppose that $1_G \in \mathscr{S}$. For $s \in \mathscr{S}$ we set $G_s = H \cap sKs^{-1}$.

Exercise 1.6.15 Let $h_1, h_2 \in H$, $k_1, k_2 \in K$, and $s \in \mathscr{S}$. Show that $h_1 s k_1 = h_2 s k_2$ if and only if there exists $x \in G_s$ such that $h_2 = h_1 x$ and $k_2 = s^{-1} x^{-1} s k_1$. Deduce that $|HsK| = |H| \cdot |K| / |G_s|$.

Let (σ, V) be a K-representation and let (ν, U) be an H-representation. We define a G_s-representation (σ_s, V_s) by setting $V_s = V$ and $\sigma_s(x) = \sigma(s^{-1} x s)$ for all $x \in G_s$, and we set

$$\mathscr{S}_0 = \{s \in \mathscr{S} : \mathrm{Hom}_{G_s}(\mathrm{Res}_{G_s}^H \nu, \sigma_s) \neq 0\}.$$

We have the following fundamental results:

- **(Mackey's formula for invariants)**

$$\mathrm{Hom}_G(\mathrm{Ind}_H^G \nu, \mathrm{Ind}_K^G \sigma) \cong \bigoplus_{s \in \mathscr{S}_0} \mathrm{Hom}_{G_s}(\mathrm{Res}_{G_s}^H \nu, \sigma_s).$$

- **(Mackey's intertwining number theorem)**

$$\dim \mathrm{Hom}_G(\mathrm{Ind}_H^G \nu, \mathrm{Ind}_K^G \sigma) = \sum_{s \in \mathscr{S}_0} \dim \mathrm{Hom}_{G_s}(\mathrm{Res}_{G_s}^H \nu, \sigma_s).$$

- **(Mackey's irreducibility criterion)**

$$\mathrm{Ind}_K^G \sigma \text{ is irreducible } \Leftrightarrow \begin{cases} \sigma \text{ is irreducible and} \\ (\forall s \in \mathscr{S} \setminus \{1_G\})\ \mathrm{Hom}_{G_s}(\mathrm{Res}_{G_s}^K \sigma, \sigma_s) = 0. \end{cases}$$

Remark 1.6.16 For a complete proof of Mackey's formula for invariants, see [19, Corollary 11.4.4]. When $H = K$ we shall revisit it in Section 1.6.5. Observe that it reduces to Frobenius reciprocity when $H = G$ and $\theta = \nu$. Moreover, both Mackey's intertwining number theorem and Mackey's irreducibility criterion are almost immediate consequences of Mackey's formula for invariants: we leave it to the reader to check the corresponding details.

Finally, we consider the counterpart of Corollary 1.6.11, namely the case when we restrict after inducing.

Theorem 1.6.17 (Mackey's lemma)

$$\mathrm{Res}^G_H \mathrm{Ind}^G_K \sigma \sim \bigoplus_{s\in\mathscr{S}} \mathrm{Ind}^H_{G_s} \sigma_s.$$

Proof See [19, Theorem 11.5.1]. □

1.6.3 The little group method of Mackey and Wigner

In this section we present a method, due to Mackey and Eugene Paul Wigner, to obtain all irreducible representations of a group G admitting a normal abelian subgroup $A \trianglelefteq G$ and satisfying a suitable condition. We first observe that G acts on $\widehat{A}$ by conjugation: if $\chi \in \widehat{A}$ and $g \in G$ we define ${}^g\chi \in \widehat{A}$ by setting

$$ {}^g\chi(a) = \chi(g^{-1}ag) \tag{1.38}$$

for all $a \in A$ (we leave it to the reader to check that the map $(g,\chi) \mapsto {}^g\chi$ is an action).

Let $\chi \in \widehat{A}$. The *inertia group* of χ is the subgroup K_χ defined by $K_\chi = \mathrm{Stab}_G(\chi) = \{g \in G : {}^g\chi = \chi\}$. Note that since A is abelian we have $A \le K_\chi$. Moreover, an *extension* of χ to K_χ is a one-dimensional K_χ-representation $\widetilde{\chi}$ such that $\chi = \mathrm{Res}^{K_\chi}_A \widetilde{\chi}$.

We recall that given a $\psi \in \widehat{K_\chi/A}$, we denote by $\overline{\psi}$ its inflation (see (1.37)).

Theorem 1.6.18 *Suppose that $\chi \in \widehat{A}$ admits an extension $\widetilde{\chi}$ to K_χ. Then*

$$\mathrm{Ind}^{K_\chi}_A \chi = \bigoplus_{\psi\in\widehat{K_\chi/A}} d_\psi(\widetilde{\chi}\otimes\overline{\psi}). \tag{1.39}$$

Moreover, if every $\chi \in \widehat{A}$ admits an extension $\widetilde{\chi}$ to K_χ, then

$$\widehat{G} = \left\{\mathrm{Ind}^G_{K_\chi}(\widetilde{\chi}\otimes\overline{\psi}) : \psi \in \widehat{K_\chi/A}, \chi \in X\right\}, \tag{1.40}$$

where X denotes a complete set of representatives of the orbits of G on $\widehat{A}$.

Proof

$$\begin{aligned}\mathrm{Ind}^{K_\chi}_A \chi &= \mathrm{Ind}^{K_\chi}_A (\chi\otimes\iota_A)\\ &= \mathrm{Ind}^{K_\chi}_A (\mathrm{Res}^{K_\chi}_A \widetilde{\chi}\otimes\iota_A)\\ &= \widetilde{\chi}\otimes\mathrm{Ind}^{K_\chi}_A \iota_A = \widetilde{\chi}\otimes\overline{\lambda}\end{aligned}$$

by Corollary 1.6.11, where $\overline{\lambda}$ denotes the inflation of the regular representation

https://doi.org/10.1017/9781009465939.002 Published online by Cambridge University Press

$\lambda = \lambda_{K_\chi/A}$ of K_χ/A. By the Peter-Weyl Theorem (cf. Theorem 1.2.36), $\lambda = \bigoplus_{\psi\in\widehat{K_\chi/A}} d_\psi \psi$ so that

$$\overline{\lambda} = \bigoplus_{\psi\in\widehat{K_\chi/A}} d_\psi \overline{\psi},$$

from which (1.39) follows.

The proof of the other statement is more involved. Let $\mathscr{S}$ be a complete set of representatives for the double cosets $K_\chi\backslash G/K_\chi$ with $1_G \in \mathscr{S}$. Set $G_s = K_\chi \cap sK_\chi s^{-1}$ and $(\widetilde{\chi}\otimes\overline{\psi})_s(x) = (\widetilde{\chi}\otimes\overline{\psi})(s^{-1}xs)$ for all $s\in\mathscr{S}$ and $x\in G_s$. Since A is abelian, we have $(\widetilde{\chi}\otimes\overline{\psi})_s(a) = {}^s\chi(a)\psi(A)$ for all $a\in A$, so that

$$\mathrm{Res}^{G_s}_A(\widetilde{\chi}\otimes\overline{\psi})_s \sim d_\psi {}^s\chi$$

which in turn implies that, for $s\neq 1_G$ $\mathrm{Res}^{K_\chi}_{G_s}(\widetilde{\chi}\otimes\overline{\psi})$ and $(\widetilde{\chi}\otimes\overline{\psi})_s$ cannot have common irreducible subrepresentations (otherwise, restricting to A would give equivalent representations, violating the fact that ${}^s\chi\neq\chi$ if $s\neq 1_G$). From Mackey's irreducibility criterion, we deduce that $\mathrm{Ind}^G_{K_\chi}(\widetilde{\chi}\otimes\overline{\psi})$ is irreducible. Finally, from Mackey's lemma we deduce that

$$\mathrm{Res}^G_{K_\chi}\mathrm{Ind}^G_{K_\chi}(\widetilde{\chi}\otimes\overline{\psi}) \sim \bigoplus_{s\in\mathscr{S}} \mathrm{Ind}^{K_\chi}_{G_s}(\widetilde{\chi}\otimes\overline{\psi})_s.$$

We leave it as an exercise to deduce, from the above expression, that ψ is uniquely determined by $\mathrm{Ind}^G_{K_\chi}(\widetilde{\chi}\otimes\overline{\psi})$. □

In the next theorem we apply the little group method in the case of a semi-direct product $G = A\rtimes H$, with A abelian. When both subgroups A and H are abelian, a simpler approach is presented in [21].

Theorem 1.6.19 *Let $G = A\rtimes H$ and suppose that A is abelian. For all $\chi\in\widehat{A}$, let $H_\chi = \mathrm{Stab}_H(\chi) = \{h\in H : {}^h\chi = \chi\}$. Then:*

(1) *the inertia group of χ is $K_\chi = A\rtimes H_\chi$;*
(2) *there exists an extension $\widetilde{\chi}$ of χ to $A\rtimes H_\chi$.*

Moreover,

$$\widehat{G} = \{\mathrm{Ind}^G_{A\rtimes H_\chi}(\widetilde{\chi}\otimes\overline{\psi}) : \chi\in X, \psi\in\widehat{H}_\chi\}, \tag{1.41}$$

where X denotes a complete set of representatives of the orbits of H on $\widehat{A}$.

Proof

(1) Given $a\in A$ and $h\in H$, we have ${}^{ah}\chi = \chi \Leftrightarrow {}^h\chi = \chi \Leftrightarrow h\in H_\chi$.
(2) Define $\widetilde{\chi}\colon A\rtimes H_\chi \to \mathbb{T}$ by setting $\widetilde{\chi}(ah) = \chi(a)$ for all $a\in A$ and $h\in H_\chi$.

We have

$$\begin{aligned}\widetilde{\chi}(a_1h_1 \cdot a_2h_2) &= \widetilde{\chi}(a_1h_1a_2h_1^{-1} \cdot h_1h_2) = \chi(a_1h_1a_2h_1^{-1}) \\ &= \chi(a_1)\chi(h_1a_2h_1^{-1}) = \chi(a_1)\chi(a_2) = \widetilde{\chi}(a_1h_1)\widetilde{\chi}(a_2h_2),\end{aligned}$$

showing that $\widetilde{\chi} \in \widehat{A \rtimes H_\chi}$. Finally, (1.41) follows immediately from (1.40). □

1.6.4 Hecke algebras

This section is based on our recent work [20] (see also [15, Chapter 13] for the particular case when the K-representation is one-dimensional).

Let G be a finite group, let $K \leq G$ be a subgroup, and let (θ, V) be a K-representation. We set $\widetilde{\mathscr{H}}(G,K,\theta)$ equal to

$$\{F\colon G \to \mathrm{End}(V) : F(k_1gk_2) = \theta(k_2^{-1})F(g)\theta(k_1^{-1}), \forall g \in G \text{ and } \forall k_1,k_2 \in K\}.$$

Given $F_1, F_2 \in \widetilde{\mathscr{H}}(G,K,\theta)$ we define their *convolution product* $F_1 * F_2\colon G \to \mathrm{End}(V)$ by setting

$$[F_1 * F_2](g) = \sum_{h \in G} F_1(h^{-1}g)F_2(h)$$

for all $g \in G$, and their scalar product as

$$\langle F_1, F_2 \rangle_{\widetilde{\mathscr{H}}(G,K,\theta)} = \sum_{g \in G} \langle F_1(g), F_2(g) \rangle_{\mathrm{End}(V)}.$$

Finally, for $F \in \widetilde{\mathscr{H}}(G,K,\theta)$ we define the *adjoint* $F^*\colon G \to \mathrm{End}(V)$ by setting

$$F^*(g) = [F(g^{-1})]^*$$

for all $g \in G$, where $[F(g^{-1})]^*$ is the adjoint of the operator $F(g^{-1}) \in \mathrm{End}(V)$.

Exercise 1.6.20 Let $F_1, F_2, F \in \widetilde{\mathscr{H}}(G,K,\theta)$. For $g \in G$, set

$$1_{\widetilde{\mathscr{H}}}(g) = \frac{1}{|K|}\mathbf{1}_K(g)\theta(g^{-1}),$$

where $\mathbf{1}_K$ denotes the characteristic function of K. Show that

- $F_1 * F_2 \in \widetilde{\mathscr{H}}(G,K,\theta)$;
- $F^* \in \widetilde{\mathscr{H}}(G,K,\theta)$;
- $(F_1 * F_2)^* = F_2^* * F_1^*$;
- $1_{\widetilde{\mathscr{H}}} \in \widetilde{\mathscr{H}}(G,K,\theta)$, and $F * 1_{\widetilde{\mathscr{H}}} = 1_{\widetilde{\mathscr{H}}} * F = F$, for all $F \in \widetilde{\mathscr{H}}(G,K,\theta)$,

and deduce that $\widetilde{\mathscr{H}}$ is a unital $*$-algebra.

https://doi.org/10.1017/9781009465939.002 Published online by Cambridge University Press

We refer to $\mathscr{H}(G,K,\theta)$ as the *Hecke algebra* associated with the triple (G,K,θ).

As in Section 1.6.2 (with $H = K$), we denote by $\mathscr{S} \subseteq G$ (with $1_G \in \mathscr{S}$) a complete set of representatives for the double K-cosets in G so that $G = \bigsqcup_{s\in\mathscr{S}} KsK$. For $s \in \mathscr{S}$ we set $K_s = K \cap sKs^{-1}$ and denote by (θ^s, V_s) the K_s-representation defined by setting $V_s = V$ and $\theta^s(x) = \theta(s^{-1}xs)$ for all $x \in K_s$. Finally, we set $\mathscr{S}_0 = \{s \in \mathscr{S} : \mathrm{Hom}_{K_s}(\mathrm{Res}^K_{K_s}\theta, \theta_s) \neq 0\}$.

Exercise 1.6.21 Choose $s \in \mathscr{S}$. For each $T \in \mathrm{Hom}_{K_s}(\mathrm{Res}^K_{K_s}\theta, \theta^s)$, define $\mathscr{L}_T : G \to \mathrm{End}(V)$ by setting

$$\mathscr{L}_T(g) = \begin{cases} \theta(k_2^{-1})T\theta(k_1^{-1}) & \text{if } g = k_1 s k_2 \text{ for some } k_1, k_2 \in K \\ 0 & \text{if } g \notin KsK. \end{cases}$$

Let $F \in \widetilde{\mathscr{H}}(G,K,\theta)$. Show that

(1) $\mathscr{L}_T$ is well defined and belongs to $\widetilde{\mathscr{H}}(G,K,\theta)$;
(2) $F(s) \in \mathrm{Hom}_{K_s}(\mathrm{Res}^K_{K_s}\theta, \theta^s)$ for all $s \in \mathscr{S}$;
(3) $F = \sum_{s\in\mathscr{S}_0} \mathscr{L}_{F(s)}$ and the nontrivial elements in this sum are linearly independent.

For $F \in \widetilde{\mathscr{H}}(G,K,\theta)$ we define $\xi(F)\colon \mathrm{Ind}^G_K V \to V[G]$ by setting

$$[\xi(F)f](g) = \sum_{h\in G} F(h^{-1}g)f(h)$$

for all $f \in \mathrm{Ind}^G_K V$ and $g \in G$. Also, for $T \in \mathrm{End}_G(\mathrm{Ind}^G_K V)$ we define $\Xi(T)\colon G \to \mathrm{End}(V)$ by setting

$$\Xi(T)(g)v = \frac{1}{|K|}[Tf_v](g),$$

for all $g \in G$ and $v \in V$, where f_v is as in (1.33).

Exercise 1.6.22 (1) Show that $\xi(F) \in \mathrm{End}_G(\mathrm{Ind}^G_K V)$ for all $F \in \widetilde{\mathscr{H}}(G,K,\theta)$.
(2) Show that $\xi(F_1 * F_2) = \xi(F_1)\xi(F_2)$ and $\xi(F^*) = \xi(F)^*$ for all $F_1, F_2, F \in \widetilde{\mathscr{H}}(G,K,\theta)$.
(3) Show that $\Xi(T) \in \widetilde{\mathscr{H}}(G,K,\theta)$ for all $T \in \mathrm{End}_G(\mathrm{Ind}^G_K V)$.
(4) Show that the normalized map $F \mapsto \frac{1}{\sqrt{|K|}}\xi(F)$ is an isometry.
(5) Show that

$$\frac{1}{|K|}\sum_{h\in G}[\lambda(h)f_{f(h)}] = f, \tag{1.42}$$

for all $f \in \mathrm{Ind}^G_K V$.

https://doi.org/10.1017/9781009465939.002 Published online by Cambridge University Press

Theorem 1.6.23 *The map* $\xi\colon \widetilde{\mathscr{H}}(G,K,\theta) \to \mathrm{End}(\mathrm{Ind}_K^G V)$ *is a* $*$*-isomorphism of unital* $*$*-algebras with inverse the map* $\Xi\colon\ \mathrm{End}_G(\mathrm{Ind}_K^G V) \to \widetilde{\mathscr{H}}(G,K,\theta)$.

Proof Having established the results in Exercise 1.6.22, we only need to check that Ξ is a right-inverse of ξ.

Given $T \in \mathrm{End}_G(\mathrm{Ind}_K^G V)$, $f \in \mathrm{Ind}_K^G$, and $g \in G$, we have

$$\begin{aligned}
[(\xi \circ \Xi(T)f]\,(g) &= \textstyle\sum_{h\in G}[\Xi(T)(h^{-1}g)]f(h)\\
&= \tfrac{1}{|K|}\textstyle\sum_{h\in G}\left[Tf_{f(h)}\right](h^{-1}g)\\
&= \tfrac{1}{|K|}\textstyle\sum_{h\in G}\left[\lambda(h)Tf_{f(h)}\right](g)\\
&= \tfrac{1}{|K|}\textstyle\sum_{h\in G}\left[T\lambda(h)f_{f(h)}\right](g)\\
&= \left[T\left(\tfrac{1}{|K|}\textstyle\sum_{h\in G}\lambda(h)f_{f(h)}\right)\right](g)\\
&= [Tf]\,(g)
\end{aligned}$$

by (1.42). This shows that $\xi(\Xi(T)) = T$, as desired. $\square$

The Hecke algebra as a subalgebra of $L(G)$**.** Let (θ,V) be a K-representation as in the first part of this section, but we now assume that θ is *irreducible*. We fix $v\in V$ with $\|v\| = 1$ and we consider an orthonormal basis $\{v_1 = v, v_2, \ldots, v_{d_\theta}\}$ of V.

We define (everything depending on the choice of the fixed vector $v \in V$):

- $\psi \in L(G)$ by setting
$$\psi(g) = \begin{cases} \frac{d_\theta}{|K|}\langle v, \theta(k)v\rangle_V & \text{if } g = k \in K\\ 0 & \text{otherwise;}\end{cases} \tag{1.43}$$
- the convolution operator $P\colon L(G) \to L(G)$ by setting $Pf = T_\psi f = f * \psi$ for all $f \in L(G)$;
- the linear operator $T\colon\ \mathrm{Ind}_K^G V \to L(G)$ by setting
$$[Tf](g) = \sqrt{d_\theta/|K|}\langle f(g), v\rangle_V$$
for all $f \in \mathrm{Ind}_K^G V$ and $g\in G$, and denote its range by
$$\mathscr{I}(G,K,\theta) = T\left(\mathrm{Ind}_K^G V\right) \subseteq L(G);$$
- the map $S\colon \widetilde{\mathscr{H}}(G,K,\theta) \to L(G)$ by setting
$$[SF](g) = d_\theta\langle F(g)v, v\rangle_V$$
for all $F \in \widetilde{\mathscr{H}}(G,K,\theta)$ and $g \in G$;
- the subspace
$$\mathscr{H}(G,K,\theta) = \{\psi * f * \psi : f \in L(G)\} \equiv \{f \in L(G) : f = \psi * f * \psi\} \le L(G). \tag{1.44}$$

https://doi.org/10.1017/9781009465939.002 Published online by Cambridge University Press

Exercise 1.6.24 (1) Show that $T \in \mathrm{Hom}_G(\mathrm{Ind}_K^G V, L(G))$ and is an isometry.

(2) Deduce that $\mathscr{I}(G,K,\theta)$ is a λ_G-invariant subspace of $L(G)$, which is G-isomorphic to $\mathrm{Ind}_K^G V$.

(3) Show that $\psi * \psi = \psi$ and $\psi^* = \psi$ and deduce that P is the orthogonal projection of $L(G)$ onto $\mathscr{I}(G,K,\theta)$.

(4) Show that $S(F) \in \mathscr{H}(G,K,\theta)$ and $S(F_1 * F_2) = S(F_2)S(F_1)$ for all $F, F_1, F_2 \in \widetilde{\mathscr{H}}(G,K,\theta)$.

(5) Show that $\frac{1}{\sqrt{d_\theta}} S$ is an isometry.

(6) Show that every $f \in \mathscr{H}(G,K,\theta)$ is supported in $\bigsqcup_{s \in \mathscr{S}_0} KsK$.

Combining the results from the above exercise we establish the following:

Theorem 1.6.25 *$\mathscr{H}(G,K,\theta)$ is an involutive subalgebra of $L(G)$, and the map $S\colon \widetilde{\mathscr{H}}(G,K,\theta) \to \mathscr{H}(G,K,\theta)$ is a $*$-anti-isomorphism of $*$-algebras.* □

1.6.5 Multiplicity-free triples and their spherical functions

This section is also based on [20] and [15, Chapter 13].

Let G be a finite group, let $K \leq G$ be a subgroup, and let $(\theta, V) \in \widehat{K}$.

Definition 1.6.26 We say that (G,K,θ) is a *multiplicity-free triple* if the algebra $\mathscr{H}(G,K,\theta)$ (cf. (1.44) and Theorem 1.6.25) is commutative.

Theorem 1.6.27 *The following conditions are equivalent:*

(1) *(G,K,θ) is a multiplicity-free triple.*

(2) *$\mathrm{Ind}_K^G \theta$ decomposes without multiplicity.*

(3) *The algebra $\widetilde{\mathscr{H}}(G,K,\theta)$ is commutative.*

(4) *The algebra $\mathrm{End}_G(\mathrm{Ind}_K^G(V))$ is commutative.*

(5) *The multiplicity of θ in $\mathrm{Res}_K^G \rho$ satisfies $m_\theta^{\mathrm{Res}_K^G \rho} \leq 1$, that is, we have*

$$\dim \mathrm{Hom}_K(V, \mathrm{Res}_K^G W) \leq 1$$

for every $(\rho, W) \in \widehat{G}$.

Proof The equivalences between (1), (2), and (3) follow from Theorem 1.6.23 and Theorem 1.6.25. The equivalence with (4) is obtained by arguing as in the proof of Theorem 1.2.60. The equivalence with the remaining condition follows from Frobenius reciprocity: we leave the details to the reader. □

The following provides a simple condition guaranteeing multiplicity-freeness:

https://doi.org/10.1017/9781009465939.002 Published online by Cambridge University Press

Proposition 1.6.28 *Suppose there exists an anti-automorphism τ of G such that $f(\tau(g)) = f(g)$ for all $f \in \mathscr{H}(G,K,\theta)$ and $g \in G$. Then (G,K,θ) is a multiplicity-free triple.*

Proof Let $f_1, f_2 \in \mathscr{H}(G,K,\theta)$ and $g \in G$. We have

$$\begin{aligned}[f_1 * f_2](g) &= \sum_{h\in G} f_1(gh) f_2(h^{-1}) \\ &= \sum_{h\in G} f_1(\tau(gh)) f_2(\tau(h^{-1})) \\ &= \sum_{h\in G} f_1(\tau(h)\tau(g)) f_2(\tau(h^{-1})) \\ &= \sum_{h\in G} f_2(\tau(h^{-1})) f_1(\tau(h)\tau(g)) \\ &= \sum_{t\in G} f_2(t^{-1}) f_1(t\tau(g)) \\ &= [f_2 * f_1](\tau(g)) = [f_2 * f_1](g).\end{aligned}$$

(setting $t = \tau(h)$ in the penultimate line). Thus $f_1 * f_2 = f_2 * f_1$, showing that $\mathscr{H}(G,K,\theta)$ is commutative. □

Remark 1.6.29 When $\theta = \iota_K$, the trivial representation of the subgroup K, we recover the case of a Gelfand pair (see Theorem 1.2.60). Note that in this context the algebra $\mathscr{H}(G,K,\iota_K)$ coincides with the algebra $\widetilde{\mathscr{H}}(G,K,\iota_K)$ and the criterion in Proposition 1.6.28 reduces to the condition of a weakly symmetric Gelfand pair (see Exercise 1.2.55).

For the rest of this section we consider a multiplicity-free triple (G,K,θ). Generalizing the case of Gelfand pairs, we show that also in this setting it is possible to develop a complete theory of spherical functions.

Definition 1.6.30 A function $\phi \in \mathscr{H}(G,K,\theta)$ is *spherical* if

$$\begin{cases} \phi * f = \lambda_{\phi,f}\phi \quad \text{for all } f \in \mathscr{H}(G,K,\theta) \\ \phi(1_G) = 1. \end{cases}$$

The proof of the next results follow the same lines of the analogous results in the setting of Gelfand pairs (cf. Section 1.2.2) and we leave it to the reader (for more details, we refer to [20, Section 4.2]; see also [19, Section 13]).

Lemma 1.6.31 *A function $\phi \in L(G) \setminus \{0\}$ is spherical if and only if*

$$\sum_{k\in K} \phi(gkh)\overline{\psi(k)} = \phi(g)\phi(h)$$

for all $g, h \in G$, where $\psi \in L(G)$ is as in (1.43). □

https://doi.org/10.1017/9781009465939.002 Published online by Cambridge University Press

Theorem 1.6.32 *Let ϕ be a spherical function and define $\Phi\colon L(G) \to \mathbb{C}$ by setting $\Phi(f)=[f*\phi](1_G)$. Then Φ is a multiplicative functional on $\mathscr{H}(G,K,\theta)$. Conversely, every multiplicative functional on $\mathscr{H}(G,K,\theta)$ comes from a spherical function as above.* $\square$

We denote by $\mathscr{J} \subseteq \widehat{G}$ the set of all irreducible G-represetations that are contained in $\mathrm{Ind}_K^G \theta$. Note that $(\rho, W) \in \mathscr{J}$ if and only if $\dim \mathrm{Hom}_K(V, \mathrm{Res}_K^G W) = 1$ (cf. Theorem 1.6.27). We then have:

Corollary 1.6.33

$$|\{\textit{spherical functions}\}| = |\mathscr{J}| = \dim \mathscr{H}(G,K,\theta).$$

Proposition 1.6.34 *Let ϕ, ϕ' be distinct spherical functions. Then*

- $\phi^* = \phi$;
- $\phi * \phi' = 0$;
- $\langle \lambda_G(g_1)\phi, \lambda_G(g_2)\phi' \rangle_{L(G)} = 0$ *for all* $g_1, g_2 \in G$. *In particular* $\phi \perp \phi'$. $\square$

Theorem 1.6.35 *Let* $U_\phi = \mathrm{span}\{\lambda_G(g)\phi : g \in G\}$. *Then*

$$\mathscr{I}(G,K,\theta) = \bigoplus_{\phi \in \mathscr{J}} U_\phi. \qquad \square$$

We denote ϕ^σ the spherical function associated with $\sigma \in \mathscr{J}$.

Definition 1.6.36 The map $\mathscr{F} : \mathscr{H}(G,K,\theta) \to \mathbb{C}^{\mathscr{J}}$ defined by setting

$$[\mathscr{F} f](\sigma) = \langle f, \phi^\sigma \rangle_{L(G)} = [f * \phi^\sigma](1_G)$$

for all $f \in \mathscr{H}$ is the *spherical Fourier transform.*

Theorem 1.6.37 (Properties of the spherical Fourier transform) *The spherical Fourier transform is an algebra isomorphism between the commutative algebras $\mathscr{H}(G,K,\theta)$ and $\mathbb{C}^{\mathscr{J}}$. Moreover, for $f, f_1, f_2 \in \mathscr{H}(G,K,\theta)$ we have:*

- *(Convolution property)*

$$\mathscr{F}[f_1 * f_2] = \mathscr{F}(f_1) \cdot \mathscr{F}(f_2);$$

- *(Inversion formula)*

$$f = \frac{1}{|G|} \sum_{\sigma \in \mathscr{J}} d_\sigma [\mathscr{F} f](\sigma) \phi^\sigma;$$

- *(Parseval identity)*

$$\langle f_1, f_2 \rangle_{L(G)} = \frac{1}{|G|} \sum_{\sigma \in \mathscr{J}} d_\sigma [\mathscr{F} f_1](\sigma) \overline{[\mathscr{F} f_1](\sigma)}. \qquad \square$$

1.7 Representation theory of $\mathrm{GL}(2,\mathbb{F}_q)$

This final section is devoted to the study of the representation theory of the general linear group $\mathrm{GL}(2,\mathbb{F}_q)$ over a finite field with q elements. It is based on part IV of our monograph [19], which sheds light on the results and the calculations in the beautiful exposition of Piatetski–Shapiro [57] by framing them in a more comprehensive theory. We start with some elementary facts on finite fields and their characters, and determining, as intermediate steps, the irreducible representations of the affine group $\mathrm{Aff}(\mathbb{F}_q)$. We also describe the subgroup structure of $\mathrm{GL}(2,\mathbb{F}_q)$ by analyzing a few important subgroups, notably the *Borel subgroup* B and the *unipotent subgroup* U, as well as its *Bruhat decomposition*. We then determine all irreducible representations and their characters of $\mathrm{GL}(2,\mathbb{F}_q)$: these are of two types, parabolic (that can be obtained by inducing up characters of the Borel subgroup) and cuspidal (whose space of U-invariant vectors is trivial).

1.7.1 Finite fields and their characters

Let $\mathbb{F}$ be a finite field. We denote by $\mathbb{F}[x]$ the ring of all polynomials in the indeterminate x with coefficients in $\mathbb{F}$, and by $\partial p(x) := n$ the *degree* of a polynomial $p(x) = a_0 + a_1x + \cdots + a_nx^n \in \mathbb{F}[x]$, $a_n \neq 0$.

Recall that the *characteristic* $\mathrm{char}(\mathbb{F})$ of $\mathbb{F}$, that is, the additive order of $1 \in \mathbb{F}$, is a prime number. Indeed, the map $\Phi\colon \mathbb{Z} \to \mathbb{F}$ defined by $\Phi(\pm n) = \pm(1+1+\cdots+1)$ for all $n \in \mathbb{N}$, is a ring homomorphism so that $\mathbb{Z}/\ker(\Phi)$ is isomorphic to $\Phi(\mathbb{Z}) \subset \mathbb{F}$. Now, $\Phi(\mathbb{Z})$, being a finite integral domain, it is itself a field (exercise). We deduce that $\ker(\Phi) = p\mathbb{Z}$ for a unique prime number p, and therefore $\mathrm{char}(\mathbb{F}) = p$.

An *extension* of $\mathbb{F}$ is a field $\mathbb{E}$ such that $\mathbb{F} \subset \mathbb{E}$. It then follows that $\mathbb{E}$ is a vector space over $\mathbb{F}$. We denote by $[\mathbb{E} : \mathbb{F}] = \dim_{\mathbb{F}} \mathbb{E}$ the *degree* of this extension.

Since $\mathbb{Z}/p\mathbb{Z} \cong \Phi(\mathbb{Z}) \subset \mathbb{F}$, we deduce that $|\mathbb{F}| = p^n$, where $n = [\mathbb{F} : \Phi(\mathbb{Z})]$.

Given an extension $\mathbb{F} \subset \mathbb{E}$, an element $\alpha \in \mathbb{E}$ is said to be *algebraic* over $\mathbb{F}$ if there exists a polynomial $p(x) \in \mathbb{F}[x]$ such that $p(\alpha) = 0$. If $\alpha \in \mathbb{E}$ is algebraic over $\mathbb{F}$, then the set $I_\alpha = \{p(x) \in \mathbb{F}[x] : p(\alpha) = 0\}$ is an ideal of $\mathbb{F}[x]$. Since $\mathbb{F}[x]$ is a *principal ideal domain*, there exists a *monic* polynomial $q(x) \in \mathbb{F}[x]$ such that $I_\alpha = q(x)\mathbb{F}[x]$. Such a polynomial $q(x)$, which is unique and irreducible (over $\mathbb{F}$), is called the *minimal polynomial* of α (over $\mathbb{F}$). Consider the ring homomorphism $\Phi\colon \mathbb{F}[x] \to \mathbb{E}$ defined by setting $\Phi(p(x)) = p(\alpha)$ for all $p(x) \in \mathbb{F}[x]$. Then $I_\alpha = \ker\Phi$ and

$$\mathbb{F}[x]/q(x)\mathbb{F}[x] \cong \Phi(\mathbb{F}[x]) = \mathbb{F}[\alpha] \leq \mathbb{E},$$

where $\mathbb{F}[\alpha]$, the subfield obtained by adjoining α to $\mathbb{F}$, satisfies $[\mathbb{F}[\alpha]:\mathbb{F}] = \partial q(x)$, the degree of the minimal polynomial of α.

Exercise 1.7.1 Let $\mathbb{F} \subset \mathbb{E}$ be an extension of fields. Show that if $[\mathbb{E}:\mathbb{F}] < \infty$, then every $\alpha \in \mathbb{E}$ is algebraic over $\mathbb{F}$.

Let $p(x) \in \mathbb{F}[x]$ of degree $\partial p(x) = n$. The smallest (i.e., of minimal degree) field extension $\mathbb{E}$ of $\mathbb{F}$ such that there exist $\alpha_1, \alpha_2, \ldots, \alpha_n \in \mathbb{E}$ and $c \in \mathbb{F}$ such that $p(x) = c(x-\alpha_1)(x-\alpha_2)\cdots(x-\alpha_n)$, is called a *splitting field* for $p(x)$ over $\mathbb{F}$.

Theorem 1.7.2 (Existence and uniqueness of finite fields)

(1) *The splitting field of any polynomial $p(x) \in \mathbb{F}[x]$ exists and is unique up to isomorphism.*
(2) *Suppose that $q = p^n$ for some integer $n \geq 1$. Then the splitting field of the polynomial $p(x) = x^q - x$ over $\mathbb{Z}/p\mathbb{Z}$ has exactly q elements, which consist of all the roots of $p(x)$.*
(3) *For every prime number p and integer $h \geq 1$ there exists a unique (up to isomorphism) finite field $\mathbb{F}_q$ of order $q = p^h$. It is isomorphic to*

$$\mathbb{F}_p[x]/\ell(x)\mathbb{F}_p[x],$$

where $\ell(x) = (x-\alpha)(x-\alpha^p)(x-\alpha^{p^2})\cdots(x-\alpha^{p^{h-1}})$ and α is any generator of the cyclic group $\mathbb{F}_q^*$.
(4) *The (multiplicative) group $\mathbb{F}_q^*$ of invertible elements of $\mathbb{F}_q$ is cyclic (of order $q-1$).*

Proof See, for instance [19, Theorem 1.1.21 and Theorem 6.3.3]. □

The *Galois group* of an extension $\mathbb{F} \subset \mathbb{E}$ is the group

$$\mathrm{Gal}(\mathbb{E}:\mathbb{F}) = \{\xi \in \mathrm{Aut}(\mathbb{E}) : \xi(x) = x \text{ for all } x \in \mathbb{F}\}$$

of automorphisms of $\mathbb{E}$ fixing all elements of $\mathbb{F}$ pointwise.

Suppose that $\mathrm{char}(\mathbb{F}) = p$. Then the map $\sigma\colon \mathbb{F} \to \mathbb{F}$ defined by $\sigma(x) = x^p$ for all $x \in \mathbb{F}$ is an automorphism of $\mathbb{F}$, called the *Frobenius automorphism* of $\mathbb{F}$. Then if $|\mathbb{F}| = p^n$, the Galois group $\mathrm{Gal}(\mathbb{F}:\mathbb{F}_p)$ is cyclic of order n, indeed it is generated by the Frobenius automorphism, and equals $\mathrm{Aut}(\mathbb{F})$.

More generally, suppose $\mathbb{E} = \mathbb{F}_{q^h} = \mathbb{F}_{p^{nh}}$ and $\mathbb{F} = \mathbb{F}_q = \mathbb{F}_{p^n}$. Then $\mathrm{Gal}(\mathbb{E}:\mathbb{F})$ is cyclic of order h, indeed generated by $\overline{\sigma} = \sigma^n$ (thus $\overline{\sigma}(x) = x^{pn} = x^q$ for all $x \in \mathbb{E}$). The *trace* and the *norm* are the maps $\mathrm{Tr}_{\mathbb{E}/\mathbb{F}}\colon \mathbb{E} \to \mathbb{F}$ and $\mathrm{N}_{\mathbb{E}/\mathbb{F}}\colon \mathbb{E} \to \mathbb{F}$ given by

$$\mathrm{Tr}_{\mathbb{E}/\mathbb{F}}(\alpha) = \sum_{k=1}^{h} \overline{\sigma}^k(\alpha) \quad\text{and}\quad \mathrm{N}_{\mathbb{E}/\mathbb{F}}(\alpha) = \prod_{k=1}^{h} \overline{\sigma}^k(\alpha) \tag{1.45}$$

https://doi.org/10.1017/9781009465939.002 Published online by Cambridge University Press

for all $\alpha \in \mathbb{E}$.

Exercise 1.7.3 Show that $\mathrm{Tr}_{\mathbb{E}/\mathbb{F}}(\alpha)$ (resp. $\mathrm{N}_{\mathbb{E}/\mathbb{F}}(\alpha)$) is indeed in $\mathbb{F}$ for every $\alpha \in \mathbb{E}$.

Theorem 1.7.4 (Hilbert Satz 90) (1) $\mathrm{Tr}_{\mathbb{E}/\mathbb{F}}$ *is a surjective* $\mathbb{F}$*-linear map from* $\mathbb{E}$ *onto* $\mathbb{F}$ *and*

$$\ker(\mathrm{Tr}_{\mathbb{E}/\mathbb{F}}) = \{\alpha - \overline{\sigma}(\alpha) : \alpha \in \mathbb{E}\}.$$

(2) $\mathrm{N}_{\mathbb{E}/\mathbb{F}}$ *yields (by restriction) a surjective homomorphism from the multiplicative group* $\mathbb{E}^*$ *of* $\mathbb{E}$ *into the multiplicative group* $\mathbb{F}^*$ *of* $\mathbb{F}$ *and*

$$\ker(\mathrm{N}_{\mathbb{E}/\mathbb{F}}) = \{\alpha\overline{\sigma}(\alpha)^{-1} : \alpha \in \mathbb{E}^*\}.$$

Quadratic extensions From now on we suppose that p is odd. An extension $\mathbb{F} \subset \mathbb{E}$ with $[\mathbb{E} : \mathbb{F}] = 2$ is called *quadratic*: it is a generalization of the familiar extension $\mathbb{R} \subset \mathbb{C}$ and the matrix representation $z = a + ib \leftrightarrow \begin{pmatrix} a & -b \\ b & a \end{pmatrix}$ for all $a, b \in \mathbb{R}$. Let $q = p^h$. Then $\mathrm{Gal}(\mathbb{F}_{q^2} : \mathbb{F}_q)$ is cyclic of order 2 and it is generated by $\overline{\sigma}$, where $\overline{\sigma}(x) = x^q$ for all $x \in \mathbb{F}_{q^2}$. Moreover, there exists an irreducible monic polynomial of degree 2 over $\mathbb{F}_q$ (in fact, there are $(q^2 - q)/2$ such) $x^2 + ax + b$, say with roots α and β.

Exercise 1.7.5 With α and β as above, show that $\overline{\sigma}(\alpha) = \beta$ (and $\overline{\sigma}(\beta) = \alpha$).

Theorem 1.7.6 *Suppose that p is odd, and $q = p^h$. Let η be a generator of the cyclic group $\mathbb{F}_q^*$ and denote by $\pm i$ the square roots of η. Then $\pm i \notin \mathbb{F}_q$ and $\{1, i\}$ is a vector space basis for $\mathbb{F}_{q^2}$ over $\mathbb{F}_q$. Moreover, $\mathbb{F}_{q^2}$ is isomorphic (as an $\mathbb{F}_q$-algebra) to the algebra $\mathbf{M}_2(\mathbb{F}_q, \eta) \subseteq \mathbf{M}_2(\mathbb{F}_q)$ consisting of all matrices of the form*

$$\begin{pmatrix} \alpha & \eta\beta \\ \beta & \alpha \end{pmatrix}$$

with $\alpha, \beta \in \mathbb{F}_q$. The isomorphism is provided by the map $\mathbf{M}_2(\mathbb{F}_q, \eta) \to \mathbb{F}_{q^2}$ given by

$$\begin{pmatrix} \alpha & \eta\beta \\ \beta & \alpha \end{pmatrix} \mapsto \alpha + i\beta \tag{1.46}$$

for all $\alpha, \beta \in \mathbb{F}_q$. Moreover $\overline{\sigma}(\alpha + i\beta) = \alpha - i\beta$ for all $\alpha, \beta \in \mathbb{F}_q$. □

The *conjugate* of an element $\alpha \in \mathbb{F}_{q^2}$ is defined as $\overline{\alpha} = \overline{\sigma}(\alpha)$. Then

$$\mathrm{Tr}_{\mathbb{F}_{q^2}/\mathbb{F}_q}(\alpha) = \alpha + \overline{\alpha} \quad \text{and} \quad \mathrm{N}_{\mathbb{F}_{q^2}/\mathbb{F}_q}(\alpha) = \alpha\overline{\alpha}$$

https://doi.org/10.1017/9781009465939.002 Published online by Cambridge University Press

for all $\alpha \in \mathbb{F}_{q^2}$. Moreover, $\alpha = \overline{\alpha}$ if and only if $\alpha \in \mathbb{F}_q$.

Characters of finite fields Let $\mathbb{F}_q$ be a finite field. An *additive character* of $\mathbb{F}_q$ is a character of the finite abelian group $(\mathbb{F}_q, +)$, that is, a map $\chi\colon \mathbb{F}_q \to \mathbb{T}$ (see Remark 1.2.29) such that $\chi(x+y) = \chi(x)\chi(y)$ for all $x, y \in \mathbb{F}_q$. The additive characters constitute a (multiplicative) abelian group, denoted by $\widehat{\mathbb{F}}_q$, called the *dual group* of $\mathbb{F}_q$.

We have the *orthogonality relations*:

$$\langle \chi, \xi \rangle_{L(\mathbb{F}_q)} \equiv \sum_{x \in \mathbb{F}_q} \chi(x)\overline{\xi(x)} = \begin{cases} q & \text{if } \chi = \xi \\ 0 & \text{otherwise,} \end{cases}$$

for all $\chi, \xi \in \widehat{\mathbb{F}}_q$.

The *principal* additive character of $\mathbb{F}_q$ is defined by setting, for all $x \in \mathbb{F}_q$,

$$\chi_{princ}(x) = \exp[2\pi i \mathrm{Tr}(x)/p], \tag{1.47}$$

where $\mathrm{Tr} = \mathrm{Tr}_{\mathbb{F}_q/\mathbb{F}_p}$ denotes the trace (cf. (1.45)) and we identify $\mathbb{F}_p$ with $\{0, 1, \ldots, p-1\}$ to compute the exponential. Since Tr is a surjective $\mathbb{F}_p$-linear map from $\mathbb{F}_q$ onto $\mathbb{F}_p$, the principal character χ_{princ} is indeed a nontrivial additive character.

Exercise 1.7.7 Let χ be a nontrivial additive character of $\mathbb{F}_q$. For each $y \in \mathbb{F}_q$ define $\chi_y\colon \mathbb{F}_q \to \mathbb{T}$ by setting

$$\chi_y(x) = \chi(xy)$$

for all $x \in \mathbb{F}_q$ (see Remark 1.2.29). Show that $\chi_y \in \widehat{\mathbb{F}}_q$, and that the map

$$\begin{array}{rccc} \Psi\colon & \mathbb{F}_q & \to & \widehat{\mathbb{F}}_q \\ & y & \mapsto & \chi_y \end{array}$$

is a group isomorphism.

Exercise 1.7.8 Show that $\widehat{\mathbb{F}}_{q^2} = \{\chi_{s,t} : s, t \in \mathbb{F}_q\}$, where

$$\chi_{s,t}(x, y) = \chi_{princ}(sx + ty) \tag{1.48}$$

for all $s, t, x, y \in \mathbb{F}_q$.

A *multiplicative character* of $\mathbb{F}_q$ is a character of the finite cyclic group $(\mathbb{F}_q^*, \cdot)$, that is, a map

$$\psi\colon \mathbb{F}_q^* \to \mathbb{T}$$

such that $\psi(xy) = \psi(x)\psi(y)$ for all $x, y \in \mathbb{F}_q^*$. The set $\widehat{\mathbb{F}}_q^*$ of all multiplicative characters is a (multiplicative) cyclic group, called the *dual group* of $\mathbb{F}_q^*$.

We have the *orthogonality relations*:

$$\langle \psi, \phi \rangle = \sum_{x \in \mathbb{F}_q^*} \psi(x)\overline{\phi(x)} = \begin{cases} q-1 & \text{if } \psi = \phi \\ 0 & \text{otherwise.} \end{cases}$$

Let x be a generator of $\mathbb{F}_q^*$. The *principal multiplicative character* of $\mathbb{F}_q^*$ associated with x is the multiplicative character ψ_{princ} defined by setting

$$\psi_{princ}(x^k) = \exp\left(\frac{2\pi i k}{q-1}\right) \tag{1.49}$$

for all $k = 1, 2, \ldots, q-1$.

Exercise 1.7.9 Show that ψ_{princ} is a generator of $\widehat{\mathbb{F}_q^*}$.

Decomposable and indecomposable characters

Let ν be a character of $\mathbb{F}_{q^2}^*$.

One says that ν is *decomposable* if there exists a character ψ of $\mathbb{F}_q^*$ such that

$$\nu(\alpha) = \psi(\alpha\overline{\alpha}) \tag{1.50}$$

for all $\alpha \in \mathbb{F}_{q^2}^*$. If this is not the case, ν is called *indecomposable*.

Moreover, the *conjugate* of ν is the character $\overline{\nu}$ defined by $\overline{\nu}(\alpha) = \nu(\overline{\alpha})$ for all $\alpha \in \mathbb{F}_{q^2}^*$.

Exercise 1.7.10 A character $\nu \in \widehat{\mathbb{F}_{q^2}^*}$ is decomposable if and only if $\nu = \overline{\nu}$.

1.7.2 Representation theory of the affine group $\mathrm{Aff}(\mathbb{F}_q)$

Let p be a prime number and let $q = p^n$. The (*general*) *affine group* (*of degree one*) over $\mathbb{F}_q$ is the subgroup $\mathrm{Aff}(\mathbb{F}_q)$ of $\mathrm{GL}(2, \mathbb{F}_q)$ defined by

$$\mathrm{Aff}(\mathbb{F}_q) = \left\{ \begin{pmatrix} a & b \\ 0 & 1 \end{pmatrix} : a \in \mathbb{F}_q^*,\ b \in \mathbb{F}_q \right\}.$$

Exercise 1.7.11 Show that the action of $\mathrm{Aff}(\mathbb{F}_q)$ on the set $\left\{ \begin{pmatrix} x \\ 1 \end{pmatrix} : x \in \mathbb{F}_q \right\}$ by left multiplication is doubly transitve.

Consider the following abelian subgroups of $\mathrm{Aff}(\mathbb{F}_q)$:

$$A = \left\{ \begin{pmatrix} a & 0 \\ 0 & 1 \end{pmatrix} : a \in \mathbb{F}_q^* \right\} \cong \mathbb{F}_q^*$$

and

$$U = \left\{ \begin{pmatrix} 1 & b \\ 0 & 1 \end{pmatrix} : b \in \mathbb{F}_q \right\} \cong \mathbb{F}_q.$$

Exercise 1.7.12 (1) The inverse of $\begin{pmatrix} a & b \\ 0 & 1 \end{pmatrix} \in \mathrm{Aff}(\mathbb{F}_q)$ is

$$\begin{pmatrix} a & b \\ 0 & 1 \end{pmatrix}^{-1} = \begin{pmatrix} a^{-1} & -a^{-1}b \\ 0 & 1 \end{pmatrix};$$

(2) the subgroup U is normal and one has

$$\mathrm{Aff}(\mathbb{F}_q) \cong U \rtimes A \equiv \mathbb{F}_q \rtimes \mathbb{F}_q^*; \tag{1.51}$$

(3) the conjugacy classes of the group $\mathrm{Aff}(\mathbb{F}_q)$ are the following:

- $\mathscr{C}_0 = \left\{ \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \right\}$;
- $\mathscr{C}_1 = \left\{ \begin{pmatrix} 1 & b \\ 0 & 1 \end{pmatrix} : b \in \mathbb{F}_q^* \right\}$;
- $\mathscr{C}_a = \left\{ \begin{pmatrix} a & b \\ 0 & 1 \end{pmatrix} : b \in \mathbb{F}_q \right\}$, where $a \in \mathbb{F}_q^*$, $a \neq 1$.

Since $\mathrm{Aff}(\mathbb{F}_q)$ is a semidirect product with an abelian normal subgroup (cf. (1.51)), we can apply the little group method (Theorem 1.6.19) in order to get a complete list of all irreducible representations of $\mathrm{Aff}(\mathbb{F}_q)$.

Exercise 1.7.13 After identifying A with the multiplicative group $\mathbb{F}_q^*$ and U with the additive group $\mathbb{F}_q$, show that the conjugacy action (cf. (1.38)) of $A \equiv \mathbb{F}_q^*$ on $\widehat{U} \equiv \widehat{\mathbb{F}_q}$ is given by

$$^{a}\chi(b) = \chi(a^{-1}b) \tag{1.52}$$

for all $\chi \in \widehat{U}, b \in \mathbb{F}_q$, and $a \in \mathbb{F}_q^*$.

Exercise 1.7.14 Denote by $\chi_0 \equiv 1$ the trivial character of U.

(1) Show that the action of A on $\widehat{U}$ has exactly two orbits, namely $\{\chi_0\}$ and $\widehat{\mathbb{F}}_q \setminus \{\chi_0\}$.
(2) Show that the stabilizer of $\chi \in \widehat{U}$ is given by

$$\mathrm{Stab}_A(\chi) = \begin{cases} \{1_A\} & \text{if } \chi \neq \chi_0 \\ A & \text{if } \chi = \chi_0. \end{cases}$$

Theorem 1.7.15 *The group* $\mathrm{Aff}(\mathbb{F}_q)$ *has exactly* $q-1$ *one-dimensional representations, obtained by associating with each* $\psi \in \widehat{A}$ *the group homomorphism* $\Psi\colon \mathrm{Aff}(\mathbb{F}_q) \to \mathbb{T}$ *defined by*

$$\Psi \begin{pmatrix} a & b \\ 0 & 1 \end{pmatrix} = \psi(a) \tag{1.53}$$

for all $\begin{pmatrix} a & b \\ 0 & 1 \end{pmatrix} \in \mathrm{Aff}(\mathbb{F}_q)$*, and one* $(q-1)$*-dimensional irreducible representation, given by*

$$\pi = \mathrm{Ind}_U^{\mathrm{Aff}(\mathbb{F}_q)} \chi, \tag{1.54}$$

where χ *is any nontrivial character of* U*.*

Proof By Exercise 1.7.14, the inertia group of the trivial character $\chi_0 \in \widehat{U}$ is $\mathrm{Aff}(\mathbb{F}_q)$. This provides the $q-1$ one-dimensional representations simply by taking any character $\psi \in \widehat{A}$. Moreover, the inertia group of any nontrivial character $\chi \in \widehat{U}$ is U since, by Exercise 1.7.14, $\mathrm{Stab}_A(\chi) = \{1_A\}$. We conclude by applying Theorem 1.6.19. $\square$

1.7.3 The general linear group $\mathrm{GL}(2, \mathbb{F}_q)$

Let $q = p^n$ with p an odd prime. We consider five important subgroups of $\mathrm{GL}(2, \mathbb{F}_q)$:

$$B = \left\{ \begin{pmatrix} \alpha & \beta \\ 0 & \delta \end{pmatrix} : \alpha, \delta \in \mathbb{F}_q^*, \beta \in \mathbb{F}_q \right\} \quad \text{(the } \textit{Borel} \text{ subgroup)}$$

$$D = \left\{ \begin{pmatrix} \alpha & 0 \\ 0 & \delta \end{pmatrix} : \alpha, \delta \in \mathbb{F}_q^* \right\} \quad \text{(the } \textit{diagonal subgroup}\text{)}$$

$$U = \left\{ \begin{pmatrix} 1 & \beta \\ 0 & 1 \end{pmatrix} : \beta \in \mathbb{F}_q \right\} \quad \text{(the } \textit{unipotent subgroup}\text{)}$$

$$Z = \left\{ \begin{pmatrix} \alpha & 0 \\ 0 & \alpha \end{pmatrix} : \alpha \in \mathbb{F}_q^* \right\} \quad \text{(the } \textit{center}\text{)}$$

$$C = \left\{ \begin{pmatrix} \alpha & \eta\beta \\ \beta & \alpha \end{pmatrix} : \alpha, \beta \in \mathbb{F}_q, (\alpha, \beta) \neq (0,0) \right\} \quad \text{(the } \textit{Cartan subgroup}\text{)},$$

where, as usual, $\mathbb{F}_q^*$ denotes the multiplicative subgroup of $\mathbb{F}_q$ consisting of all nonzero elements, and η is a generator of $\mathbb{F}_q^*$; cf. Theorem 1.7.6

We have the following:

- $B = U \rtimes D \cong \mathrm{Aff}(\mathbb{F}_q) \times Z$.
- $U = [B, B] = B'$ is abelian.
- Let $w = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \in \mathrm{GL}(2, \mathbb{F}_q)$, then (*Bruhat decomposition*):

$$\mathrm{GL}(2, \mathbb{F}_q) = B \sqcup BwU = B \sqcup UwB = B \sqcup BwB.$$

- $\mathrm{Aff}(\mathbb{F}_q) = U \rtimes A$.

Exercise 1.7.16 Show that $|\mathrm{GL}(2, \mathbb{F}_q)| = (q^2-1)(q^2-q) = q(q+1)(q-1)^2$.

https://doi.org/10.1017/9781009465939.002 Published online by Cambridge University Press

Theorem 1.7.17 *The following table describes the conjugacy classes of the group* $\mathrm{GL}(2,\mathbb{F}_q)$.

TYPE	*RE*	*NC*	*NE*	*NAME*	*C(RE)*
(a)	$\begin{pmatrix}\lambda & 0\\ 0 & \lambda\end{pmatrix}$, $\lambda \neq 0$	$q-1$	*1*	*central*	$\mathrm{GL}(2,\mathbb{F}_q)$
(b_1)	$\begin{pmatrix}\lambda_1 & 0\\ 0 & \lambda_2\end{pmatrix}$, $\lambda_1 \neq \lambda_2$	$\frac{(q-1)(q-2)}{2}$	q^2+q	*hyperbolic*	D
(b_2)	$\begin{pmatrix}\lambda & 1\\ 0 & \lambda\end{pmatrix}$, $\lambda \neq 0$	$q-1$	q^2-1	*parabolic*	ZU
(b_3)	$C \setminus Z$	$\frac{q(q-1)}{2}$	q^2-q	*elliptic*	C

where

- *TYPE indicates* type *of the conjugacy class*
- *RE indicates* representative element*: for each (conjugacy) class we indicate a representative element;*
- *NC indicates* number of conjugacy classes*: this equals the number of representative elements;*
- *NE indicates the* number of elements *in each class;*
- *NAME indicates the* denomination *of this type of class;*
- $C(RE)$ *indicates the* centralizer in $\mathrm{GL}(2,\mathbb{F}_q)$ of the representative element.

Proof We leave it as an exercise. The main point is to observe that two matrices are conjugate if and only if they have the same *minimal* and *characteristic* polynomials (for *nonscalar* matrices, the characteristic polynomial suffices). □

The representation theory of the Borel subgroup B may be then easily deduced from Theorem 1.7.15 and the isomorphism

$$B = \mathrm{Aff}(\mathbb{F}_q) \times Z \cong \mathrm{Aff}(\mathbb{F}_q) \times \mathbb{F}_q^*,$$

which gives (see Theorem 1.2.46)

$$\widehat{B} = \widehat{\mathrm{Aff}(\mathbb{F}_q)} \boxtimes \widehat{Z} \cong \widehat{\mathrm{Aff}(\mathbb{F}_q)} \boxtimes \widehat{\mathbb{F}_q^*}.$$

Theorem 1.7.18 *The Borel subgroup B has:*

https://doi.org/10.1017/9781009465939.002 Published online by Cambridge University Press

- $(q-1)^2$ *one-dimensional representations, namely* $\Psi_1 \boxtimes \Psi_2$*, where* Ψ_1 *is a one-dimensional representation of* $\mathrm{Aff}(\mathbb{F}_q)$ *and* $\Psi_2 \in \widehat{Z}$*;*
- $q-1$ *irreducible* $(q-1)$*-dimensional representations, namely* $\pi \boxtimes \Psi$*, where* π *is the unique irreducible representation of* $\mathrm{Aff}(\mathbb{F}_q)$ *of dimension* $q-1$ *and* $\Psi \in \widehat{Z}$*.*

Using the correspondence between characters of $\mathrm{Aff}(\mathbb{F}_q)$ *and those of* $\mathbb{F}_q^*$*, given by* (1.53)*, these representations are explicitly given by*

$$(\Psi_1 \boxtimes \Psi_2)\begin{pmatrix}\alpha & \beta\\ 0 & \delta\end{pmatrix} = \psi_1(\alpha\delta^{-1})\psi_2(\delta) \quad \textit{for all} \begin{pmatrix}\alpha & \beta\\ 0 & \delta\end{pmatrix} \in B,$$

with $\psi_1, \psi_2 \in \widehat{\mathbb{F}_q^*}$*, and*

$$(\pi \boxtimes \Psi)\begin{pmatrix}\alpha & \beta\\ 0 & \delta\end{pmatrix} = \pi\begin{pmatrix}\alpha\delta^{-1} & \beta\delta^{-1}\\ 0 & 1\end{pmatrix}\psi(\delta) \quad \textit{for all} \begin{pmatrix}\alpha & \beta\\ 0 & \delta\end{pmatrix} \in B,$$

with $\psi \in \widehat{\mathbb{F}_q^*}$*.*

Notation Rearranging the *parametrization* we set

$$\chi_{\psi_1,\psi_2}\begin{pmatrix}\alpha & \beta\\ 0 & \delta\end{pmatrix} = \psi_1(\alpha)\psi_2(\delta) \quad \text{and } \chi_{\psi,\psi} = \psi(\det(b))$$

for all $\psi_1, \psi_2, \psi \in \widehat{\mathbb{F}_q^*}$ and $\begin{pmatrix}\alpha & \beta\\ 0 & \delta\end{pmatrix}, b \in B$. Also, we shall make no distinction between $\mathrm{Res}^B_D \chi_{\psi_1,\psi_2}$ and χ_{ψ_1,ψ_2}.

If $\chi \in \widehat{D}$, let ${}^w\chi$ be defined by ${}^w\chi(d) = \chi(wdw)$ for all $w \in D$. Then ${}^w\chi_{\psi_1,\psi_2} = \chi_{\psi_2,\psi_1}$.

1.7.4 Representations of $\mathrm{GL}(2,\mathbb{F}_q)$

In the first part of this section we determine the irreducible representations of $\mathrm{GL}(2,\mathbb{F}_q)$ that may be obtained by inducing up the characters of the Borel subgroup B. First we give a general principle.

Proposition 1.7.19 *Let G be a group and $N \trianglelefteq G$ a normal subgroup. Then the map* $(\rho, U) \mapsto (\widetilde{\rho}, U)$ *defined by*

$$\widetilde{\rho}(gN)u = \rho(g)u \tag{1.55}$$

for all $g \in G$ and $u \in U$, is a bijection between the set of all G-representations (ρ, U) *such that* $\mathrm{Res}^G_N \rho$ *is trivial and the set of all G/N-representations.*

Proof We leave it to the reader to check that $\widetilde{\rho}$ is well defined, and that the inverse map is given by the inflation. □

https://doi.org/10.1017/9781009465939.002 Published online by Cambridge University Press

Exercise 1.7.20 Let H be a finite group and denote by H' its derived subgroup. Deduce from the previous proposition that there exists a bijective correspondence between the set of all (irreducible) one-dimensional representations of H and the characters of H/H'.

Proposition 1.7.21 *Let (ρ, V) be an irreducible representation of a group G. Then, if $H \leq G$ and $V^{H'}$ denotes the subspace of all H'-invariant vectors in V (this is called the* Jacquet module*), we have*

$$V^{H'} \neq \{0\} \Leftrightarrow \text{ there exists } \chi\widehat{H} \text{ such that } d_\chi = 1 \text{ and } \rho \text{ is contained in } \operatorname{Ind}_H^G \chi.$$

Proof The H-representation $(\operatorname{Res}_H^G \rho, V^{H'})$ when restricted to H' is trivial. Therefore it yields a representation of the abelian group H/H' which is a direct sum of characters. By Exercise 1.7.20 it therefore corresponds to a direct sum of one-dimensional H-representations.

If $V^{H'} \neq 0$, then there exists a one-dimensional H-representation χ such that $(\chi, \mathbb{C}) \preceq (\operatorname{Res}_H^G \rho, V^{H'}) \preceq (\operatorname{Res}_H^G \rho, V)$. By Frobenius reciprocity we deduce that $\rho \preceq \operatorname{Ind}_H^G \chi$. □

Notation

- We set $G = \mathrm{GL}(2, \mathbb{F}_q)$.
- If χ is a one-dimensional representation of B, we denote by $(\widehat{\chi}, V)$ the G-representation $(\operatorname{Ind}_B^G \chi, \operatorname{Ind}_B^G \mathbb{C})$ (note that $\dim V = q+1$).
- Since $D = B/B'$, there exists a bijection between one-dimensional representations of B and characters of D: given $\chi \in \widehat{D}$, we denote by ${}^w\chi$ the one-dimensional representation of B corresponding to the character $\chi \in \widehat{D}$.

Proposition 1.7.22 *Let χ be a one-dimensional representation of B. Then*

$$(\operatorname{Res}_B^G \widehat{\chi}, V^U) \sim (\chi \oplus {}^w\chi, \mathbb{C}^2).$$

Proof By our definitions, $V^U \leq \operatorname{Ind}_B^G \mathbb{C}$ and, by the Bruhat decomposition, $f \in V^U$ only depends on $f(1_G)$ and $f(w)$. We then leave it to the reader to compute the corresponding matrix coefficients (for more details see [19, Proposition 14.5.5]) and complete the proof. □

Notation For $\psi \in \widehat{\mathbb{F}_q^*}$, we define a one-dimensional G- representation by setting

$$\widehat{\chi}_\psi^0(g) = \psi(\det(g))$$

for all $g \in G$.

Theorem 1.7.23 (1) *Let $\psi_1, \psi_2, \xi_1, \xi_2 \in \widehat{\mathbb{F}_q^*}$. If $\psi_1 \neq \psi_2$, then $\widehat{\chi}_{\psi_1,\psi_2}$ is an irreducible G -representation of dimension $q+1$. Moreover,*

$$\widehat{\chi}_{\psi_1,\psi_2} \sim \widehat{\chi}_{\xi_1,\xi_2} \Leftrightarrow \{\psi_1, \psi_2\} = \{\xi_1, \xi_2\}.$$

https://doi.org/10.1017/9781009465939.002 Published online by Cambridge University Press

In particular,

$$\left\{\widehat{\chi}_{\psi_1,\psi_2} : \psi_1 \neq \psi_2 \in \widehat{\mathbb{F}_q^*}\right\}$$

are $\frac{(q-1)(q-2)}{2}$ *pairwise nonequivalent irreducible representations of* G.

(2) *For each* $\psi \in \widehat{\mathbb{F}_q^*}$ *there exists an irreducible* G*-representation* $\widehat{\chi}_\psi^1$ *of dimension* q *such that*

$$\widehat{\chi}_{\psi,\psi} = \widehat{\chi}_\psi^0 \oplus \widehat{\chi}_\psi^1.$$

Moreover,

$$\left\{\widehat{\chi}_\psi^1 : \psi \in \widehat{\mathbb{F}_q^*}\right\} \text{ and } \left\{\widehat{\chi}_\psi^0 : \psi \in \widehat{\mathbb{F}_q^*}\right\}$$

is a set of $(q-1)$ *pairwise nonequivalent* q*-dimensional* G*-representations, and the set of* all *one-dimensional* G*-representations, respectively.*

Proof By the Bruhat decomposition $G = B \sqcup BwB$ we have that $S = \{1_G, w\}$ is a complete set of representatives for the double coset $B\backslash G/B$. Moreover $G_w = B \cap wBw = D$ and Mackey's formula for invariants gives, for all one-dimensional representations χ, ξ of B:

$$\mathrm{Hom}_G(\widehat{\chi},\widehat{\xi}) = \mathrm{Hom}_B(\chi,\xi) \oplus \mathrm{Hom}_D(\mathrm{Res}^B_D \chi, {}^w\xi) = \mathrm{Hom}_B(\chi,\xi) \oplus \mathrm{Hom}_D(\chi, {}^w\xi).$$

We deduce that

- if $\xi = \chi$ and $\chi \neq {}^w\chi$, then $\widehat{\chi}$ is irreducible;
- if $\chi \neq {}^w\chi$, $\xi \neq {}^w\xi$ and $\{\chi, {}^w\chi\} \neq \{\xi, {}^w\xi\}$, then $\widehat{\chi} \not\sim \widehat{\xi}$;
- if $\chi = {}^w\chi$, then $\dim \mathrm{Hom}_G(\widehat{\chi},\widehat{\chi}) = 2$ so $\widehat{\chi} = \sigma_1 \oplus \sigma_2$, with $\sigma_1, \sigma_2 \in \widehat{G}$.

We observe that $\widehat{\chi}_\psi^0 \preceq \widehat{\chi}_{\psi,\psi}$: if $f(g) = \overline{\psi(\det g)}$, with $g \in G$, we have

$$f(gb) = \overline{\psi(\det gb)} = \overline{\psi(\det gb)} = \overline{\psi(\det g)\psi(\det b)} = \overline{\chi_{\psi,\psi}(b)} f(g)$$

for all $b \in B$. As a consequence,

$$[\widehat{\chi}_{\psi,\psi}(g)f](g_0) = f(g^{-1}g_0) = \widehat{\chi}_\psi^0 f(g_0),$$

so there exists $\widehat{\chi}_\psi^1 \preceq \widehat{\chi}$ such that $\widehat{\chi} = \widehat{\chi}_\psi^0 \oplus \widehat{\chi}_\psi^1$. We leave it to the reader to check that if $\psi \neq \phi$, then $\widehat{\chi}_\psi^1 \not\sim \widehat{\chi}_\phi^1$. □

Definition 1.7.24 A G-representation (ρ, V) is called *cuspidal* if the space $V^U = \{v \in V : \rho(u)v = v, \forall u \in U\}$ of all U-invariant vectors is trivial. We denote by $\mathrm{Cusp} = \mathrm{Cusp}(\mathrm{GL}(2,\mathbb{F}_q)) \subset \widehat{\mathrm{GL}(2,\mathbb{F}_q)}$ a complete set of pairwise nonequivalent *irreducible* cuspidal representations.

Theorem 1.7.25 *Let $\chi \in \widehat{U}$ be a nontrivial character. Then $\mathrm{Ind}_U^G \chi$ is multiplicity-free, does not depend on χ, and its decomposition is*

$$\mathrm{Ind}_U^G \chi = \left[\bigoplus_{\psi\in\widehat{\mathbb{F}_q^*}} \widehat{\chi}_\psi^1\right] \oplus \left[\bigoplus_{\psi_1\neq\psi_2\in\widehat{\mathbb{F}_q^*}} \widehat{\chi}_{\psi_1,\psi_2}\right] \oplus \left[\bigoplus_{\rho\in\mathrm{Cusp}} \rho\right]$$

so that $\mathrm{Ind}_U^G \chi$ contains all the irreducible G-representations of dimension greater than one.

Proof We have that $U \trianglelefteq B$ and $B = \sqcup_{d\in D} dU = \sqcup_{d\in D} UdU$ so that from the Bruhat decomposition we get

$$G = B \sqcup UwB = \left(\bigsqcup_{d\in D} UdU\right) \sqcup \left(\bigsqcup_{d\in D} UwdU\right).$$

We deduce the following facts.

- $\mathscr{S} = D \sqcup wD$ is a complete set of representatives for the double U-cosets in G.
- $dUd^{-1} \cap U = U$ and $wdUd^{-1}w \cap U = \{1_G\}$ for all $d \in D$.
- $\mathscr{S}_0 = Z \sqcup wD = \mathscr{S} \setminus (D \setminus Z)$.
- $f \in \mathscr{H}(G,K,\psi)$ vanishes on $\sqcup_{d\in D\setminus Z} dU$; equivalently f is supported in $\sqcup_{s\in Z\sqcup wD} UsU$.

Define $\tau\colon G \to G$ by setting

$$\tau\begin{pmatrix}\alpha & \beta\\ \gamma & \delta\end{pmatrix} = \begin{pmatrix}\delta & \beta\\ \gamma & \alpha\end{pmatrix}$$

for all $\begin{pmatrix}\alpha & \beta\\ \gamma & \delta\end{pmatrix} \in G$. It is immediate to check that τ is an involutive anti-automorphism of G. We claim that, if $f \in \mathscr{H}(G,U,\chi)$, then $f^\tau = f$, where $f^\tau(g) = f(\tau(g))$ for all $g \in G$.

Indeed, $\mathrm{supp}(f) \subseteq U(Z \sqcup wD)U$ and it obvious that $\tau|_U$ (resp. $\tau|_Z$) is the identity on U (resp. on Z). Since

$$\tau(wd) = \tau\left(\begin{pmatrix}0 & 1\\ 1 & 0\end{pmatrix}\begin{pmatrix}\alpha & 0\\ 0 & \beta\end{pmatrix}\right) = \tau\left(\begin{pmatrix}0 & \beta\\ \alpha & 0\end{pmatrix}\right) = \begin{pmatrix}0 & \beta\\ \alpha & 0\end{pmatrix} = wd$$

for all $d = \begin{pmatrix}\alpha & 0\\ 0 & \beta\end{pmatrix} \in D$, the claim follows.

We deduce from Proposition 1.6.28, that the Hecke algebra $\mathscr{H}(G,U,\chi)$ is commutative and therefore (cf. Theorem 1.6.27) $\mathrm{Ind}_U^G \chi$ is multiplicity-free. By transitivity of induction we have

$$\mathrm{Ind}_U^G \chi = \mathrm{Ind}_{\mathrm{Aff}(\mathbb{F}_q)}^G \mathrm{Ind}_U^{\mathrm{Aff}(\mathbb{F}_q)} \chi = \mathrm{Ind}_{\mathrm{Aff}(\mathbb{F}_q)}^G \pi \tag{1.56}$$

which implies that also $\mathrm{Ind}_{\mathrm{Aff}(\mathbb{F}_q)}^G \pi$ is multiplicity-free.

The explicit decomposition of $\mathrm{Ind}_U^G \chi$ follows from the following observations.

- The multiplicity of $\widehat{\chi}_\psi^1$ and $\widehat{\chi}_{\psi_1,\psi_2}$ in $\mathrm{Ind}_U^G \chi$ is one, for all $\psi_1, \psi_2, \psi \in \widehat{\mathbb{F}_q^*}$ (exercise; hint: use (1.56)).
- If ρ is a cuspidal representation, then $\mathrm{Res}_{\mathrm{Aff}(\mathbb{F}_q)}^G \rho$ cannot contain a one-dimensional representation of $\mathrm{Aff}(\mathbb{F}_q)$. Otherwise, the restriction to U (which equals the derived subgroup of $\mathrm{Aff}(\mathbb{F}_q)$) of a one-dimensional representation of $\mathrm{Aff}(\mathbb{F}_q)$ being trivial would provide nontrivial U-invariant vectors, contradicting ρ being cuspidal. It follows that $\mathrm{Res}_{\mathrm{Aff}(\mathbb{F}_q)}^G \rho = m\pi$ for some integer $m \geq 1$. But, by Frobenius reciprocity and (1.56),

$$1 \geq m_\rho^{\mathrm{Ind}_U^G \chi} = m \geq 1,$$

showing that the multiplicity of ρ in $\mathrm{Ind}_U^G \chi$ is exactly one. $\square$

https://doi.org/10.1017/9781009465939.002 Published online by Cambridge University Press

References

[1] J. L. Alperin and R. B. Bell, *Groups and Representations*, Graduate Texts in Mathematics, **162**. Springer-Verlag, New York, 1995.

[2] R. A. Bailey, *Association Schemes: Designed Experiments, Algebra and Combinatorics*. Cambridge Studies in Advanced Mathematics **84**, Cambridge University Press, 2004.

[3] E. Bannai and T. Ito, *Algebraic Combinatorics*, Benjamin, Menlo Park, CA, 1984.

[4] E. Bannai, E. Bannai, T. Ito and R. Tanaka, *Algebraic Combinatorics*, De Gruyter Series in Discrete Mathematics and Applications volume 5, De Gruyter 2021.

[5] L. Bartholdi and R. I. Grigorchuk, On parabolic subgroups and Hecke algebras of some fractal groups. *Serdica Math. J.* **28** (2002), no. 1, 47–90.

[6] K. P. Bogart, An obvious proof of Burnside's lemma, *Amer. Math. Monthly* **98** (1991), no. 10, 927–928.

[7] A. Borodin and G. Olshanski, *Representations of the Infinite Symmetric Group*. Cambridge Studies in Advanced Mathematics, **160**. Cambridge University Press, Cambridge, 2017.

[8] A. E. Brouwer, A. M. Cohen and A. Neumaier, *Distance-Regular Graphs*. Ergebnisse der Mathematik und ihrer Grenzgebiete (3) [Results in Mathematics and Related Areas (3)], **18**. Springer-Verlag, Berlin, 1989.

[9] D. Bump and D. Ginzburg, Generalized Frobenius–Schur numbers, *J. Algebra* **278** (2004), no. 1, 294–313.

[10] W. Burnside, *Theory of Groups of Finite Order*, Cambridge University Press, 1897.

[11] P. J. Cameron, *Permutation Groups*. London Mathematical Society Student Texts, **45**. Cambridge University Press, Cambridge, 1999.

[12] P. J. Cameron and J. H. van Lint, *Designs, Graphs, Codes and their Links*. London Mathematical Society Student Texts, **22**. Cambridge University Press, Cambridge, 1991.

[13] T. Ceccherini-Silberstein, F. Scarabotti and F. Tolli, Trees, wreath products and finite Gelfand pairs, *Adv. Math.*, **206** (2006), no. 2, 503–537.

[14] T. Ceccherini-Silberstein, F. Scarabotti and F. Tolli, Finite Gelfand pairs and their applications to probability and statistics, *J. Math. Sci. (N.Y.)* **141** (2007), no. 2, 1182–1229.

[15] T. Ceccherini-Silberstein, F. Scarabotti and F. Tolli, *Harmonic Analysis on Finite Groups: Representation Theory, Gelfand Pairs and Markov Chains*. Cambridge Studies in Advanced Mathematics **108**, Cambridge University Press, Cambridge, 2008.

[16] T. Ceccherini-Silberstein, F. Scarabotti and F. Tolli, *Representation Theory of the Symmetric Groups: the Okounkov–Vershik Approach, Character Formulas, and Partition Algebras.* Cambridge Studies in Advanced Mathematics **121**, Cambridge University Press, Cambridge, 2010.

[17] T. Ceccherini-Silberstein, A. Machí, F. Scarabotti and F. Tolli, Induced representations and Mackey theory. Functional analysis. *J. Math. Sci. (N.Y.)* **156** (2009), no. 1, 11–28.

[18] T. Ceccherini-Silberstein, F. Scarabotti and F. Tolli, *Representation Theory and Harmonic Analysis of Wreath Products of Finite Groups*, London Mathematical Society Lecture Note Series **410**, Cambridge University Press, Cambridge, 2014.

[19] T. Ceccherini-Silberstein, F. Scarabotti and F. Tolli, *Discrete Harmonic Analysis: Representations, Number Theory, Expanders, and the Fourier Transform*. Cambridge Studies in Advanced Mathematics, **172**, Cambridge University Press, Cambridge, 2018.

[20] T. Ceccherini-Silberstein, F. Scarabotti and F. Tolli, *Gelfand Triples and their Hecke Algebras — harmonic analysis for multiplicity-free induced representations of finite groups. With a foreword by Eiichi Bannai*, Lecture Notes in Mathematics **2267**, Springer, Cham, 2020.

[21] T. Ceccherini-Silberstein, F. Scarabotti and F. Tolli, *Representation theory of finite group extensions. Clifford theory, Mackey obstruction, and the orbit method*, Springer Monographs in Mathematics, Springer, Cham, 2022.

[22] P. Corsini and V. Leoreanu, *Applications of Hyperstructure Theory*, Springer, 2003.

[23] D. D'Angeli and A. Donno, Self-similar groups and finite Gelfand pairs, *Algebra Discrete Math.* (2007), no. 2, 54–69.

[24] D. D'Angeli and A. Donno, A group of automorphisms of the rooted dyadic tree and associated Gelfand pairs, *Rend. Semin. Mat. Univ. Padova* **121** (2009), 73–92.

[25] Ph. Delsarte, *An algebraic approach to the association schemes of coding theory*, Philips Res. Rep. Suppl. No. 10 (1973).

[26] P. Diaconis, *Group Representations in Probability and Statistics.* IMS Hayward, CA, 1988.

[27] P. Diaconis and M. Shahshahani, Generating a random permutation with random transpositions, *Z. Wahrsch. Verw. Geb.*, **57** (1981), 159–179.

[28] P. Diaconis and M. Shahshahani, Time to reach stationarity in the Bernoulli–Laplace diffusion model, *SIAM J. Math. Anal.* **18** (1987), no. 1, 208–218.

[29] J. Dieudonné, *Treatise on Analysis* Vol. VI. Pure and Applied Mathematics, 10-VI. Academic Press, Inc. New York-London, 1978.

[30] Ch. F. Dunkl, The measure algebra of a locally compact hypergroup, *Trans. Amer. Math. Soc.* **179** (1973), 331–348.

[31] Ch. F. Dunkl, Structure hypergroups for measure algebras, *Pacific J. Math.* **47** (1973), 413–425.

[32] Ch. F. Dunkl, Spherical functions on compact groups and applications to special functions. Symposia Mathematica, Vol. XXII (Convegno sull'Analisi Armonica e Spazi di Funzioni su Gruppi Localmente Compatti, INDAM, Rome, 1976), pp. 145–161. Academic Press, London, 1977.

[33] Ch. F. Dunkl, Orthogonal functions on some permutation groups, *Proc. Symp. Pure Math.* **34**, Amer. Math. Soc., Providence, RI, (1979), 129–147.

[34] H. Dym and H. P. McKean, *Fourier Series and Integrals*, Probability and Mathematical Statistics, No. 14. Academic Press, New York-London, 1972.

[35] P. Ehrenfest and T. Ehrenfest, Über zwei bekannte Einwände gegen das Boltzmannsche H-Theorem. *Physikalische Zeitschrift* **8** (1907), 311–314.

[36] J. Faraut, Analyse harmonique sur les paires de Guelfand et les espaces hyperboliques, CIMPA lecture notes (1980).

[37] A. Figà-Talamanca, Note del Seminario di Analisi Armonica, A.A. 1990–91, Università di Roma "La Sapienza".

[38] A. Figà-Talamanca and C. Nebbia, *Harmonic Analysis and Representation Theory for Groups Acting on Homogeneous Trees*, London Mathematical Society Lecture Note Series **162**. Cambridge University Press, Cambridge, 1991.

[39] W. Fulton and J. Harris, *Representation Theory. A First Course*, Springer-Verlag, New York, 1991.

[40] I. M. Gelfand, Spherical functions in symmetric Riemann spaces, *Doklady Akad. Nauk SSSR (N.S.)* **70**, (1950); [Collected papers, Vol. II, Springer (1988) 31–35].

[41] C. D. Godsil, *Algebraic Combinatorics*. Chapman and Hall Mathematics Series. Chapman & Hall, New York, 1993.

[42] C. Godsil and G. Royle, *Algebraic Graph Theory*. Graduate Texts in Mathematics **207**, Springer-Verlag, New York, 2001.

[43] R. I. Grigorchuk, Just infinite branch groups, in *New Horizons in Pro-p Groups* (ed. Marcus de Sautoy, Dan Segal and Aner Shalev), 121–179, Progr. Math. **184**, Birkhäuser Boston, Boston, MA, 2000.

[44] S. Helgason, *Groups and Geometric Analysis: Integral Geometry, Invariant Differential Operators, and Spherical Functions*. Mathematical Surveys and Monographs, **83**. American Mathematical Society, Providence, RI, 2000.

[45] D. A. Holton and J. Sheehan, *The Petersen Graph*. Australian Mathematical Society Lecture Series **7**, Cambridge University Press, Cambridge, 1993.

[46] I. M. Isaacs, *Character Theory of Finite Groups*, Corrected reprint of the 1976 original [Academic Press, New York]. Dover Publications, Inc., New York, 1994.

[47] M. R. Jerrum, Computational Pólya theory, in *Surveys in Combinatorics, 1995* (P. Rowlinson, ed.), London Math. Soc. Lecture Notes **218**, Cambridge University Press, Cambridge, 1995, pp. 103–118.

[48] R. J. Jewett, Spaces with an abstract convolution of measures, *Advances in Math.* **18** (1975), no. 1, 1–101.

[49] J. H. van Lint and R.M. Wilson, *A Course in Combinatorics*. Second edition. Cambridge University Press, Cambridge, 2001.

[50] I. G. Macdonald, *Symmetric Functions and Hall Polynomials.* Second edition. With contributions by A. Zelevinsky. Oxford Mathematical Monographs. Oxford Science Publications. The Clarendon Press, Oxford University Press, New York, 1995.

[51] F. J. MacWilliams and N. J. A. Sloane, *The Theory of Error-Correcting Codes*, Vol. I and II. North-Holland Mathematical Library, Vol. 16. North-Holland Publishing Co., Amsterdam-New York-Oxford, 1977.

[52] M. A. Naimark and A. I. Stern, *Theory of Group Representations*, Springer-Verlag, New York, 1982.

[53] A. F. Nikiforov, S. K. Suslov and V. B. Uvarov, *Classical Orthogonal Polynomials of a Discrete Variable*. Springer Series in Computational Physics. Springer-Verlag, Berlin, 1991.

[54] P. M. Neumann, A lemma that is not Burnside's, *Math. Sci.* **4** (1979), no. 2, 133–141.

[55] A. Okounkov and A. M. Vershik, A new approach to representation theory of symmetric groups. *Selecta Math. (N.S.)* **2** (1996), no. 4, 581–605.

[56] F. Peter and H. Weyl, Die Vollständigkeit der primitiven Darstellungen einer geschlossenen kontinuierlichen Gruppe, *Math. Ann.*, **97** (1927), 737–755.

[57] I. I. Piatetski-Shapiro, *Complex Representations of* $\mathrm{GL}(2,K)$ *for Finite Fields K*. Contemporary Mathematics, **16**. American Mathematical Society, Providence, R.I., 1983.

[58] M. Reed and B. Simon, *Methods of Modern Mathematical Physics. II. Fourier Analysis and Self-Adjointness.* Academic Press [Harcourt Brace Jovanovich, Publishers], New York-London, 1975.

[59] J. Saxl, On multiplicity-free permutation representations, in *Finite Geometries and Designs* (ed. P. J. Cameron, J. W. P. Hrschfeld and D. R. Hughes), pp. 337–353, London Math. Soc. Lecture Notes Series, **49**, Cambridge University Press, 1981.

[60] F. Scarabotti, Time to reach stationarity in the Bernoulli-Laplace diffusion model with many urns, *Adv. in Appl. Math.* **18** (1997), no. 3, 351–371.

[61] F. Scarabotti and F. Tolli, Harmonic analysis on a finite homogeneous space, *Proc. Lond. Math. Soc.*(3) **100** (2010), no. 2, 348–376.

[62] F. Scarabotti and F. Tolli, Fourier analysis of subgroup-conjugacy invariant functions on finite groups, *Monatsh. Math.* **170** (2013), 465–479.

[63] F. Scarabotti and F. Tolli, Hecke algebras and harmonic analysis on finite groups, *Rend. Mat. Appl.* (7) **33** (2013), no. 1-2, 27–51.

[64] F. Scarabotti and F. Tolli, Induced representations and harmonic analysis on finite groups, *Monatsh. Math.* **181** (2016), no. 4, 937–965.

[65] J. P. Serre, *Linear Representations of Finite Groups*, Graduate Texts in Mathematics **42**. Springer-Verlag, New York-Heidelberg, 1977.

[66] B. Simon, *Representations of Finite and Compact Groups*, American Math. Soc., 1996.

[67] D. Stanton, An introduction to group representations and orthogonal polynomials, in *Orthogonal Polynomials* (P. Nevai Ed.), 419–433, Kluwer Academic Dordrecht, 1990.

[68] S. Sternberg, *Group Theory and Physics*, Cambridge University Press, Cambridge, 1994.

[69] A. Terras, *Fourier Analysis on Finite Groups and Applications*. London Mathematical Society Student Texts **43**. Cambridge University Press, Cambridge, 1999.

[70] H. Wielandt, *Finite Permutation Groups*, Academic Press, New York-London, 1964.

[71] J. Wolf, *Harmonic Analysis on Commutative Spaces*. Mathematical Surveys and Monographs **142**. American Mathematical Society, Providence, RI, 2007.

[72] E. M. Wright, Burnside's lemma: a historical note, *J. Comb. Theory* (B), **30** (1981), 89–90.

[73] P.-H. Zieschang, *Theory of Association Schemes*, Springer Monographs in Mathematics. Springer-Verlag, Berlin, 2005.